CENTRO UNIVERSITÁRIO EUROAMERICANO – UNIEURO
PRÓ-REITORIA E PÓS-GRADUAÇÃO, PESQUISA E EXTENSÃO
COORDENAÇÃO DE PÓS-GRADUAÇÃO LATO SENSU
MBA EM GOVERNANÇA DE TI

CARLOS EDUARDO MIRANDA ZOTTMANN

JEFFERSON COLOMBO BARBOSA XAVIER

LIANA QUEIROS FONTELLES TURQUETTI

AVALIAÇÃO DE MATURIDADE DAS MEDIDAS DE CONTINUIDADE DA INFRAESTRUTURA DE TI DO PROCESSO ELETRÔNICO NO STJ, SOB A ÓTICA DO PROCESSO DS4 DO COBIT

Brasília, março/2010

CARLOS EDUARDO MIRANDA ZOTTMANN

JEFFERSON COLOMBO BARBOSA XAVIER

LIANA QUEIROS FONTELLES TURQUETTI

AVALIAÇÃO DE MATURIDADE DAS MEDIDAS DE CONTINUIDADE DA INFRAESTRUTURA DE TI DO PROCESSO ELETRÔNICO NO STJ, SOB A ÓTICA DO PROCESSO DS4 DO COBIT

Trabalho de conclusão de curso apresentado como pré-requisito parcial para a conclusão do curso de MBA em Governança de TI do Centro Universitário Euroamericano – Unieuro.

Orientador: Professor Dr. José Gonçalo dos Santos

Brasília, março/2010

CARLOS EDUARDO MIRANDA ZOTTMANN

JEFFERSON COLOMBO BARBOSA XAVIER

LIANA QUEIROS FONTELLES TURQUETTI

AVALIAÇÃO DE MATURIDADE DAS MEDIDAS DE CONTINUIDADE DA INFRAESTRUTURA DE TI DO PROCESSO ELETRÔNICO NO STJ, SOB A ÓTICA DO PROCESSO DS4 DO COBIT

Esta monografia foi julgada adequada à obtenção do grau de Especialista em *Governança de TI* e aprovada em sua forma final pelo curso de Pós-graduação Lato Sensu em *Governança de TI* do Centro Universitário UNIEURO.

Data de aprovação:

Banca Examinadora

Prof. Dr. José Gonçalo dos Santos – Orientador
Centro Universitário UNIEURO

Prof.ª Msc. Kerlla de Souza Luz
Centro Universitário UNIEURO

Prof. Msc. Francisco Handrick Tomaz da Costa
Centro Universitário UNIEURO

RESUMO

O Superior Tribunal de Justiça iniciou um ousado projeto de transformação dos autos dos processos judiciais do formato tradicional, em papel, para o formato eletrônico, onde todas as peças processuais serão armazenadas em arquivos de computador. Tal transformação altera completamente a função que a Tecnologia da Informação atualmente exerce no sistema judicial, voltada ao registro e divulgação de informações de acompanhamento, ou mesmo do conteúdo de certas peças que não apresentam valor legal, para uma função mais ativa, uma vez que tais peças somente existirão, e, portanto terão validade legal, em meio digital. Os requisitos de segurança de acesso, autenticidade e integridade dos autos, bem como de sua disponibilidade para acesso às partes interessadas, ora restritos ao meio físico em que se encontram armazenados, serão agora aplicados diretamente sobre o sistema informatizado e sobre a infraestrutura tecnológica que suportam o novo Processo Judicial Eletrônico, multiplicados pelas novas facilidades de acesso em função de sua disponibilização via Internet. Em função desta modificação de cenário, diversas medidas foram tomadas referentes à continuidade desta infraestrutura, de forma a proporcionar um maior índice de disponibilidade dos processos judiciais em meio eletrônico, evitando assim alongamentos desnecessários nos prazos judiciais. A análise de maturidade destas medidas frente ao processo DS4 do COBIT pretende estabelecer o grau de eficácia das mesmas em função do objetivo pretendido, ou seja, um índice de disponibilidade satisfatório às exigências da prestação jurisdicional.

Palavras-Chave: Processo Judicial Eletrônico – Lei 11.419/06 – Continuidade de TI – COBIT – Superior Tribunal de Justiça.

ABSTRACT

The Superior Court of Justice began a daring project of transformation of the judicial processes from the traditional format, in paper, to an electronic format, where all the processual pieces will be stored in computer archives. Such a transformation alters completely the role that the Information Technology plays at present in the judicial system, focused on registering and publicizing judicial informations, or even registering the content of certain pieces that do not present legal value, to a more active role, once that such pieces will only exist, and so will have legal validity, in a digital environment. The requisites of access security, authenticity and entirety of the processes, as well as their availability to interested parts, currently limited to the physical environment in which they are stored, will now be applied to the computerized system and to the technological infrastructure that support the new digital process, multiplied by the new access methods now offered through the Internet. As an outcome of this new scenario, several measures were taken regarding infrastructure continuity, in order to provide higher availability rates of the judicial processes in this new electronic environment, avoiding unnecessary delays. The analysis of the maturity of these measures compared to the best practices defined by the COBIT DS4 Process intends to establish their efficiency degree regarding the pretended objective, in other words, an availability rate that stands up to the demands of the judicial system.

Keywords: Judicial Eletronic Process – 11.419/06 Act. – IT Continuity – COBIT – Superior Court of Justice.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BCP	Business Continuity Plan
BSC	Balanced Scorecard
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CNJ	Conselho Nacional de Justiça
COBIT	Control Objectives for Information and Related Technology
COSO	Comitee of Sponsoring Organizations
eSCM-SP	eSourcing Capability Model for Service Providers
Gbps	Gigabits por segundo
GCN	Gestão da Continuidade do Negócio
GTI	Governança da Tecnologia da Informação
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISACF	Information Systems Audit and Control Foundation
ISO	International Organization for Standardization
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
LTO	Linear Tape Open
PCN	Plano de Continuidade de Negócios
PDCA	Plan, Do, Check, Act
PMBOK	Project Management Body of Knowledge
PTR	Plano de tratamento de risco
RACI	Responsable, accountable, consulted, Informed
SEI	Software Engineering Institute
SGSI	Sistema de Gerenciamento de Segurança da Informação
SoA	Statements of Applicability
STJ	Superior Tribunal de Justiça
SW-CMM	Capability Maturity Model for Software
TI	Tecnologia da Informação
WORM	Write Once Read Many

SUMÁRIO

1. INTRODUÇÃO

1.1. Problema e Justificativa.

O Poder Judiciário brasileiro vem constantemente sendo alvo de críticas da sociedade no que se refere à agilidade da prestação jurisdicional. Muito embora o próprio rito aplicado aos julgamentos contribua largamente para a percepção de morosidade da justiça reinante na sociedade, rito este que prevê diversas possibilidades de recursos às decisões judiciais, tanto na própria instância onde o julgamento ocorreu quanto em instâncias superiores, há espaço para a agilização dos processos mediante a análise e melhoria dos procedimentos atualmente adotados.

Diversas ações vêm sendo adotadas com este propósito, desde ações organizacionais, visando melhorias de processos para a agilização dos julgamentos e a redução do passivo de processos judiciais, até modificações na legislação, tal como a promulgação da Lei 11.419/06, que disciplina a informatização do Processo Judicial Eletrônico e estabelece as bases legais para sua implantação.

Como exemplos de ações organizacionais, podemos citar as ações de Gestão e Planejamento do Poder Judiciário que vêm sendo capitaneadas pelo Conselho Nacional de Justiça (2009) que, dentre outras, estabeleceu um conjunto de metas a serem alcançadas pelos Tribunais de 1° e 2° graus e Tribunais Superiores, a saber:

1. Desenvolver e/ou alinhar planejamento estratégico plurianual (mínimo de 05 anos) aos objetivos estratégicos do Poder Judiciário, com aprovação no Tribunal Pleno ou Órgão Especial.
2. Identificar os processos judiciais mais antigos e adotar medidas concretas para o julgamento de todos os distribuídos até 31/12/2005 (em 1º, 2º grau ou tribunais superiores).
3. Informatizar todas as unidades judiciárias e interligá-las ao respectivo tribunal e à rede mundial de computadores (internet).
4. Informatizar e automatizar a distribuição de todos os processos e recursos.
5. Implantar sistema de gestão eletrônica da execução penal e mecanismo de acompanhamento eletrônico das prisões provisórias.

6. Capacitar o administrador de cada unidade judiciária em gestão de pessoas e de processos de trabalho, para imediata implantação de métodos de gerenciamento de rotinas.
7. Tornar acessíveis as informações processuais nos portais da rede mundial de computadores (internet), com andamento atualizado e conteúdo das decisões de todos os processos, respeitado o segredo de justiça.
8. Cadastrar todos os magistrados como usuários dos sistemas eletrônicos de acesso a informações sobre pessoas e bens e de comunicação de ordens judiciais (Bacenjud, Infojud, Renajud).
9. Implantar núcleo de controle interno.
10. Implantar o processo eletrônico em parcela de suas unidades judiciárias.

A Meta n° 10 é particularmente afetada pela Lei 11.419/06, sendo que o Superior Tribunal de Justiça - STJ vem desenvolvendo esforços para alcançar os objetivos por ela traçados, implementando o Processo Judicial Eletrônico, que consiste basicamente em três grandes etapas:

1. Digitalização do acervo de processos atualmente em tramitação no STJ;
2. Geração das peças processuais originárias do STJ já em meio digital;
3. Desenvolvimento e fornecimento de sistemas informatizados que permitam às instâncias inferiores a digitalização de seus processos, com o consequente envio dos mesmos ao STJ já em meio digital.

A implementação do Processo Judicial Eletrônico significa que os Processos Judiciais não mais existirão em meio físico, mas tão somente em meio digital. Tal fato traz diversas consequências à área de Tecnologia da Informação, desde o desenvolvimento de todos os sistemas necessários, passando pela divulgação e treinamento de usuários, até modificações na infraestrutura necessária para a execução dos sistemas e para o armazenamento das peças processuais em meio digital, respeitados os requisitos de disponibilidade, integridade e confidencialidade.

1.2. Objetivos do Trabalho

1.2.1. Objetivo Geral

Este trabalho visa avaliar as medidas de continuidade da infraestrutura implantadas pela Secretaria de Tecnologia da Informação do STJ para dar suportar ao Processo Judicial Eletrônico, à luz das melhores práticas recomendadas pelo COBIT, em seu processo DS4.

1.2.2. Objetivos Específicos

- Apresentar os impactos na infraestrutura de TI do STJ motivados pela adoção do Processo Judicial Eletrônico;
- Apresentar as medidas de continuidade adotadas pelo Superior Tribunal de Justiça para atender aos requisitos de integridade e disponibilidade do Processo Judicial Eletrônico; e
- Apresentar um diagnóstico de maturidade das medidas de continuidade à luz do processo DS4 e dos objetivos de controle propostos pelo COBIT.

1.3. Estrutura da Monografia

No Capítulo 1, é abordado o cenário que possibilita a adoção do Processo Judicial Eletrônico pelo Superior Tribunal de Justiça, apresentação dos objetivos específicos e gerais do trabalho e a sua estruturação.

No Capítulo 2, é apresentada a fundamentação teórica sendo abordados conceitos relativos a Governança de TI, modelos de melhores práticas, ISO/IEC 27001, framework COBIT e modelo de maturidade da Governança de TI.

No Capítulo 3, são apresentadas a composição do Poder Judiciário brasileiro e atribuições do STJ, a evolução da legislação e o Processo Judicial Eletrônico, a Lei 11.419/06 , o fim da era papel no STJ, o impacto do Processo Judicial Eletrônico na área de Tecnologia da Informação e as medidas de continuidade adotadas no âmbito do Processo Judicial Eletrônico.

No Capítulo 4, é apresentada a metodologia da pesquisa.

No Capítulo 5, são apresentados os resultados da análise dos dados obtidos a partir da aplicação dos questionários de maturidade.

No Capítulo 6, é apresentada a conclusão do trabalho.

2. GOVERNANÇA DE TI: MELHORES PRÁTICAS, AUDITORIA E MÉTRICAS DE AVALIAÇÃO

Neste capítulo iremos apresentar a definição e os objetivos da Governança de TI, e um resumo dos principais modelos de melhores práticas que compõe seu "framework".

Em seguida trataremos em detalhe dos modelos que relacionam-se com as melhores práticas da continuidade da infraestrutura de TI difundidos no mercado, a International Organization for Standardization (ISO/IEC 27001:2005), e o *Control Objectives for Information and related Technology* (COBIT).

Mais adiante aprofundaremos a analise do modelo COBIT, especificamente no processo DS4, responsável por Garantir a Continuidade dos Serviços e finalizando, apresentaremos o modelo de maturidade proposto pelo *IT Governance Institute* para avaliar a maturidade dos processos de TI.

2.1. Governança da Tecnologia da Informação (GTI)

A Governança da Tecnologia da Informação (GTI), tradução do termo em inglês *IT Governance*, é definida como um conjunto de estruturas e processos que visa garantir que a Tecnologia da Informação suporte e maximize adequadamente os objetivos e estratégias de negócio da organização (IT GOVERNANCE INSTITUTE, 2009).

Outra definição afirma que a GTI consiste em um ferramental para a especificação dos direitos de decisão e responsabilidade, visando encorajar comportamentos desejáveis no uso da TI (WEILL e ROSS, 2004) (*apud* FERNANDES e ABREU, 2006, p. 11).

Os objetivos das práticas de Governança de TI visam garantir que as expectativas de TI estão atendidas, seu desempenho é medido, os seus recursos são geridos e seus riscos são mitigados (IT GOVERNANCE INSTITUTE, 2009).

O objetivo principal da GTI é alinhar a TI aos requisitos do negócio. Este alinhamento tem como base a continuidade do negócio, o atendimento às estratégias do negócio, e o atendimento a marcos de regulação externos (FERNANDES e ABREU, 2006, p.13).

Para alcançar a Governança da Tecnologia da Informação as organizações utilizam modelos de gestão, que se aplicados asseguram a conformidade com as melhores práticas de processos e segurança da informação.

Um modelo de Governança de TI possibilita: controlar – medir e auditar – a execução e a qualidade dos serviços; acompanhar contratos internos e externos; e criar condições para o eficaz exercício da gestão de TI, com base em conceitos consolidados de qualidade. É importante considerar que enquanto a Gestão de TI possui uma orientação interna e focada no presente, a Governança de TI é orientada para o negócio, com foco no futuro.

Existem disponíveis vários modelos de melhores práticas para a Governança de TI, cada um deles possuindo um foco específico, o que em muitos casos leva as organizações a adotar vários desses modelos em conjunto, visando aproveitar o que cada um tem a oferecer de melhor. Com a combinação desses modelos pode-se obter um “framework’ de governança de TI.

A seguir serão descritos, de forma resumida, alguns dos principais modelos adotados no “framework” de governança de TI e suas principais características:

- BSC (*Balanced Scorecard)* é um sistema de gestão estratégica utilizado para alinhar as atividades do negócio a visão e a estratégia da organização. O modelo é baseado em quatro perspectivas (financeira, cliente, processos internos e aprendizado e crescimento), que tem como objetivos a tradução da estratégia em termos operacionais, o alinhamento da organização à estratégia e a transformação da estratégia em um processo contínuo, endereçado a todos da organização (BALANCED SCORECARD INSTITUTE, 2009);
- CMMI (*Capability Maturity Model Integration*) é uma abordagem de melhoria de processo e habilidades organizacionais, com foco no gerenciamento do desenvolvimento, aquisição e manutenção de produtos e serviços. (SOFTWARE ENGINEERING INSTITUTE, 2009);

- COBIT (*Control Objectives for Information and related Technology*) é um modelo que integra e institucionaliza boas práticas de planejamento e organização, aquisição e implementação, entrega e suporte, e monitoramento e avaliação do desempenho de TI, com foco mais acentuado no controle que na execução;
- eSCM-SP é um modelo orientado exclusivamente para operações de outsourcing, que atende não somente a serviços de TI, mas a outros serviços que usam a tecnologia da informação. O modelo é composto por 84 práticas organizadas ao longo do ciclo de vida do sourcing, agrupadas por área de capacidade e nível de capacidade;
- ISO/IEC 27001:2005 é um código de prática para o estabelecimento, a implementação, a operação, o monitoramento, a revisão, a manutenção e a melhoria do sistema de gerenciamento da segurança da informação de uma organização;
- ITIL (*Information Technology Infrastructure Library*) é um conjunto de melhores práticas com foco na operação e na infraestrutura de TI. A adoção adequada das práticas do ITIL leva a organização a um grau de qualidade que permita o uso eficiente e eficaz dos seus sistemas de informação e da sua infraestrutura de TI, sempre com o foco no atendimento das necessidades dos clientes e usuários;
- PMBOK (*Project Management Body of Knowledge*) é um guia onde se descreve as principais áreas de conhecimento e as melhores práticas dentro da área de gerência de projetos. Outro objetivo do PMBOK é a padronização de termos utilizados em gerência de projetos; e
- SEIS SIGMA é um sistema que visa a melhoria do desempenho do negócio através da melhoria do desempenho de processos, tendo como meta um processo que apresente um rendimento de 99,9997% de resultados do processo isentos de defeitos.

2.2. ISO/IEC 27001:2005

Em 2008 o STJ deciciu implementar um Sistema de Gestão de Segurança da Informação – SGSI. O projeto teve como objetivo estabelecer a conformidade com a norma ISO/IEC 27001:2005 no ambiente do CPD do STJ, preparando esse ambiente para a certificação.

A decisão de adotar a norma se deu por várias razões, dentre elas o fato da ISO/IEC 27001 ser um padrão reconhecido mundialmente, por oferecer um conjunto de argumentos organizados para gestão de segurança da informação, aumentar a credibilidade das ações de segurança que passam a ter um selo de qualidade, demonstrar a maturidade em relação a segurança da informação e por fim, ajudar no atendimento à legislação vigente.

Por essa razão, aprofundaremos o estudo da norma, conhecendo sua estrutura e os requisitos necessários à certificação.

2.2.1. ESTRUTURA DA NORMA

> A norma ISO/IEC 27001:2005 é a evolução natural da BS 7799-2:2002, norma britânica que trata da definição de requisitos para um Sistema de Segurança da Informação. O padrão foi incorporado pela The International Organization for Standardization (ISO – Organização não governamental de âmbito internacional com sede na Suíça, que cuida do estabelecimento de padrões internacionais para certificação em diversas áreas) (BASTOS e CAUBIT, 2009, p. 18).

A ISO organiza as normas afins em famílias que mantêm uma estrutura similar em qualquer tema a ser tratado. A família ISO 27000 não foge à regra, como podemos ver a seguir:

- **ISO/IEC 27000 – Fundamentos e Vocabulário**: norma que apresenta a estrutura do conjunto de normas da família e estabelece um rol de conceitos básicos sobre o assunto a que a norma se refere, neste caso segurança da informação;

- **ISO/IEC 27001 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos**: norma que especifica os requisitos para um sistema de gestão de segurança da informação, que podem ser utilizados pelas organizações para aplicação interna, para certificação ou para fins contratuais. Ela esta focada na eficácia do sistema de gestão de segurança da informação em manter o nível de segurança requerido para atender as partes interessadas e gerenciar a segurança da informação de acordo com os riscos do negócio. Esta norma pode ser utilizada para avaliar a conformidade pelas partes interessadas internas e externas, ou seja, é a parte da norma que apresenta requisitos para as auditorias; e
- **ISO/IEC 27002 – Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão de Segurança da Informação – Código de Prática para Gestão da Segurança da Informação**: norma que apresenta um guia de boas práticas em segurança da informação, orientando e apresentando recomendações para implementação dos controles do ANEXO A da norma ISO 27001.

Existem outras normas da família ISO 27000, a saber: ISO 27003 (Guia de Implementação), ISO 27004 (Métricas e medidas), ISO 27005 (Gestão de Riscos), ISO 27006 (Requisitos de Acreditação para Certificação em Segurança da Informação), ISO 27007 (Orientações para Gestão de Auditorias de Sistemas de Segurança da Informação) e ISO 27008 (Orientações para Auditores de Sistema de Segurança da Informação). Detalhamos apenas as duas normas que têm maior relevância para nossa pesquisa.

Segundo (BASTOS e CAUBIT, 2009, p. 18) a norma ISO 27001:2005 é a norma BS7799-2:2002 revisada, com melhorias e adaptações, contemplando o ciclo PDCA de melhorias e a visão de processos que as normas de sistemas de gestão atuais já incorporaram.

A figura 2.1, mostra o ciclo PDCA (*Plan-Do-Check-Act*), ou seja planejar, fazer, checar e agir, também conhecido como ciclo de Deming, que é sugerido para a execução e implementação desta norma.

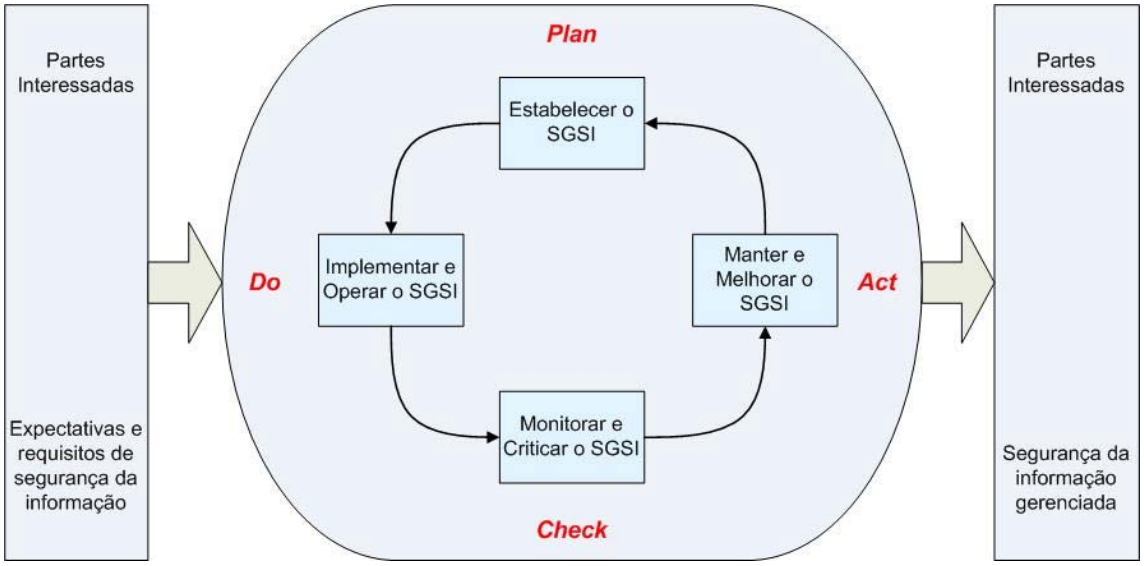

Figura 2.1 – Modelo PDCA aplicado ao SGSI.

Fonte : NBR ISO/IEC 27001:2006, pg. 3 - adaptado

Na estrutura do PDCA, cada uma das atividades pode ser descrita da seguinte forma:

- ***Plan* (Estabelecimento do SGSI)**: estabelecer um plano de trabalho que pode ser um cronograma, um gráfico ou um conjunto de orientações. Definir metas e métodos. As metas podem decorrer do plano para casos de recursos limitados ou o plano pode objetivar o alcance da meta. Definindo a política do SGSI, os objetivos, os processos e procedimentos relevantes para a gestão de riscos e a melhoria da segurança da informação para entregar resultados conforme as políticas globais da organização e seus objetivos de negócio;
- ***Do* (Implementação e operação do SGSI)**: esta etapa significa implementar e operar as regras estabelecidas na política do SGSI, os controles, os processos e procedimentos. As tarefas devem ser realizadas exatamente como previstas no plano, devendo-se coletar dados para verificação do funcionamento do processo conforme o previsto. Nesta etapa é essencial o treinamento da equipe nas práticas de trabalho definidas no plano;
- ***Check* (Monitoramento e análise crítica do SGSI)**: esta etapa significa monitorar e revisar o SGSI. A partir dos dados coletados durante a execução, comparar os resultados alcançados com a meta planejada. Avaliar e, onde aplicável, medir o desempenho de um processo de acordo com as regras estabelecidas na política do SGSI, com os objetivos e experiência prática, relatando os resultados para os gestores efetuarem a revisão ou análise crítica do sistema de gestão; e

- ***Act* (Manutenção e melhoria do SGSI)**: esta é a etapa onde os desvios são detectados e a equipe atuará no sentido de fazer correções de tal modo que o problema não volte a ocorrer. Esta atuação é metódica e busca alcançar a melhoria contínua do SGSI.

Conforme afirmação de Bastos e Caubit (2009, p. 26), a gestão da segurança da informação traz benefícios para as organizações que implementarem o SGSI, mesmo que o principal objetivo não seja a obtenção da certificação junto a um organismo certificador credenciado. Entre outros benefícios específicos, podemos citar os mais comuns:

- Fortalecer a percepção de segurança perante os usuários, clientes, fornecedores, sociedade, funcionários, acionistas, agências reguladoras e judiciário;
- Integração da segurança da informação com os objetivos do negócio;
- Segurança da informação demonstrável e monitorada;
- Linguagem única internacional com padrões da família ISO 27000;
- Atendimento a requisitos jurídicos e regulatórios;
- Fortalecimento na cadeia de valor de segurança e tecnologia da informação;
- Aprimoramento da gestão de segurança da informação na organização, devido à aplicação do ciclo do PDCA;
- Melhoria no poder de negociação de Riscos Operacionais e Seguros; e
- Fortalecimento da área e profissionais de segurança da informação da organização.

As normas são organizadas em 11 seções, onde são apresentados os controles de segurança. Na norma ISO 27001, estes controles são apresentados no ANEXO A e, na norma ISO 27002, os controles são apresentados a partir da seção 5, como podemos ver na figura 2.2

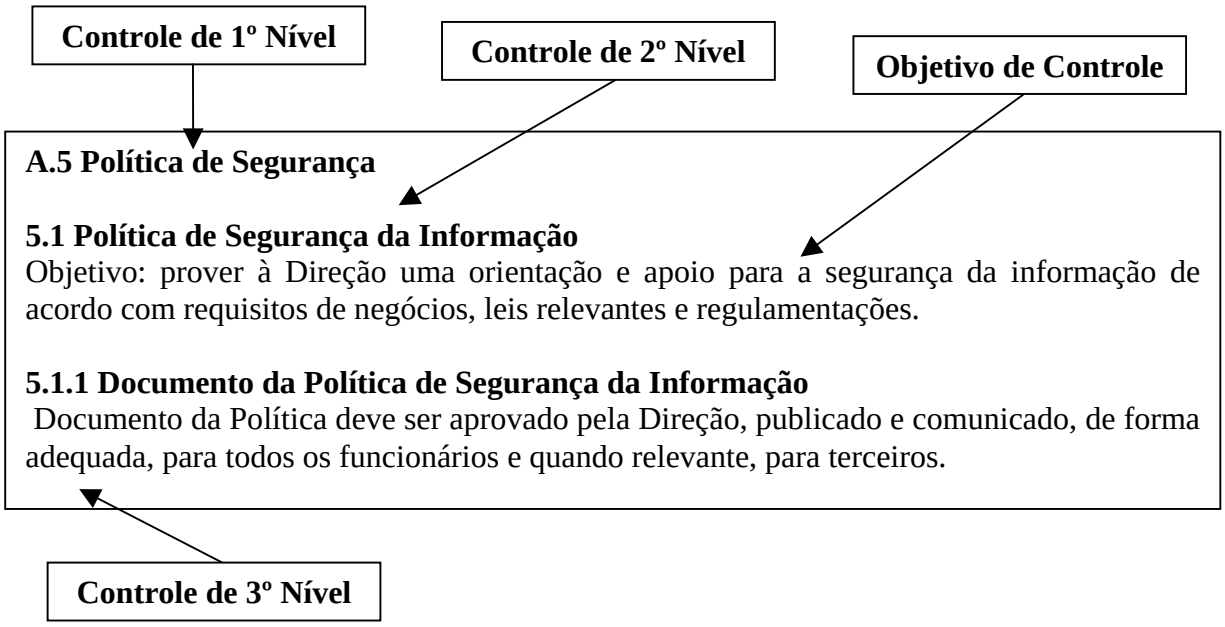

Figura 2.2 – Exemplo de controle de segurança.

Fonte : BASTOS e CAUBIT (2009, p. 28) - adaptado

São 11 controles de 1º nível, onde são apresentadas as principais categorias de segurança da informação; 39 controles de 2º nível e seus respectivos objetivos de controle; e 133 controles de 3º nível. Na norma ISO 27001, os controles são apresentados com seus respectivos objetivos e as condições mínimas para auditoria ou verificação de sua implementação. Já na norma ISO 27002, os controles são descritos seguindo a estrutura abaixo:

- **Controle**: define qual o controle específico para atender ao objetivo de controle.
- **Diretrizes de implementação**: contém informações mais detalhadas para apoiar a implementação do controle e atender ao objetivo de controle. As diretrizes de implementação são genéricas e pretendem atender a qualquer tipo de organização, porém é possível que tais diretrizes não se apliquem e seja necessário buscar uma forma de implementação mais adequada.
- **Informações adicionais**: apresenta informações complementares às diretrizes de implementação e, em alguns casos, exemplos ou considerações legais ou referências a outras normas.

2.2.2. Objetivo de Controle A.14 – Gestão da Continuidade do Negócio (GCN)

No âmbito da ISO 27001 o objetivo de controle que trata da Gestão da Continuidade de Negócios é o A.14, classificado como mandatório devido à sua importância para a continuidade da operação da organização.

Segundo Ramos (2006, p. 156) o Plano de Continuidade de Negócios (PCN ou BCP – *Business Continuity Plan*) é constituído de uma série de procedimentos e medidas que terão por objetivo minimizar as perdas decorrentes de um desastre[1], ou seja, de um evento de grandes proporções em termos de impacto. A criação, a manutenção e a incorporação deste plano à organização fazem parte de um processo maior, chamado Gestão da Continuidade de Negócios.

> O principal objetivo da Gestão da Continuidade do Negócio (GCN) é evitar que ocorra a interrupção das atividades do negócio e proteger processos críticos contra efeitos de falhas operacionais internas ou de terceiros, ou desastres significativos, assegurando a retomada em tempo hábil do funcionamento dos sistemas (BASTOS e CAUBIT, 2009, p. 100).

O objetivo de controle A.14 possui cinco controles de segundo nível, os quais transcrevemos abaixo:

- **A.14.1.1 – Incluindo segurança da informação no processo de gestão de continuidade de negócio**.

  Controle: um processo de gestão deve ser desenvolvido e mantido para assegurar a continuidade do negócio por toda organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio da organização.

[1]O fator-chave que define se um evento é um desastre ou não, para o âmbito de um PCN, é o tempo de parada que o evento causará nos processos críticos da organização.

- **A.14.1.2 – Continuidade de negócios e análise/avaliação de risco**

  Controle: devem ser identificados os eventos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e as conseqüências para a segurança da informação;

- **A.14.1.3 – Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação**

  Controle: os planos devem ser desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio;

- **A.14.1.4 – Estrutura do plano de continuidade do negócio**

  Controle: uma estrutura básica do plano de continuidade do negócio deve ser mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção;

- **A.14.1.5 – Testes, manutenção e reavaliação dos planos de continuidade do negócio**

  Controle: os planos de continuidade do negócio devem ser testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

O controle de segundo nível A.14.1.1 tem exigência de procedimento documentado. Há exigência de evidências comprobatórias em todos os controles de terceiro nível.

Para a efetividade do objetivo de controle A.14, devem ser realizadas análises e avaliações de riscos e impactos nos negócios buscando o alinhamento dos planos de continuidade às reais necessidades da organização.

A estrutura de um conjunto de planos que contemplem ações de contingência, recuperação de desastres, continuidade operacional, administração da crise, retorno à normalidade das atividades após a recuperação do funcionamento normal dos ativos deve ser montada e um planejamento de testes para comprovar a eficácia dos planos de continuidade

do negócio deve ser elaborado e executado. É preciso que os planos sejam mantidos atualizados e aderentes à política de segurança da informação.

Os principais planos a serem elaborados são os seguintes:

- **Plano de Administração da Crise**: seu conteúdo está voltado aos procedimentos do Gestor do Plano de Continuidade do Negócio (PCN). Descrição completa das equipes, responsabilidades e atribuições antes, durante e depois de um incidente. Gerencia todas as atividades de resposta, contingência e recuperação;
- **Plano de Resposta a Incidentes**: seu conteúdo está voltado aos procedimentos de contenção e/ou limitação dos danos ocasionados pela ocorrência de um incidente, que poderá levar ao acionamento dos Planos de Continuidade dos Processos/Componentes do Negócio e Planos de Recuperação de Desastres de Ativos. É responsável por antever, sempre que possível, as possibilidades de ocorrência de incidentes de segurança e tem como objetivo estabelecer por meio de contramedidas adequadas, para cada risco eminentemente detectado, as ações corretivas (de prevenção e preparação);
- **Plano de Continuidade Operacional**: seu conteúdo está voltado aos procedimentos de continuidade dos Processos/Componentes do Negócio. O plano possui todos os procedimentos de continuidade dos processos/componentes, recursos de hardware e software, sob guarda de grupos funcionais específicos;
- **Plano de Recuperação de Desastres**: seu conteúdo está voltado aos procedimentos de recuperação/restauração dos ativos. O plano possui todos os procedimentos de recuperação dos ativos, recursos de hardware e software, sob guarda de grupos funcionais específicos;
- **Plano de Retorno à Normalidade**: seu conteúdo esta voltado aos procedimentos (fluxo) para o retorno a normalidade. Tanto pode ser referente a um Plano de Continuidade Operacional como a um Plano de Resposta a Incidente. São os procedimentos que devem ser efetuados para que o Processo/Componentes de Negócio volte à normalidade, não estado mais em “situação de contingência”.

A certificação na norma ISO 27001 usualmente envolve um processo de auditoria em duas fases:

- Na primeira fase é feita uma revisão (de mesa), também denominada de pré-auditoria, da existência e completude de documentação chave como a política de segurança da organização, plano de tratamento de risco (PTR) e declaração de aplicabilidade ("*Statements of Applicability* – SoA"), documento que formalizará os objetivos e controles aplicáveis e pertinentes a cada companhia que pretenda obter a certificação de seus Sistemas de Gestão da Segurança da Informação;

- Na segunda fase é feito um detalhamento, com auditoria em profundidade envolvendo a existência e efetividade do SGSI declarados no PTR e SoA, bem como a documentação de suporte.

A renovação do certificado envolve revisões periódicas e redeclaração confirmando que o SGSI continua operando como desejado.

O STJ obteve a certicação ISO 27001 em agosto de 2008, tendo renovado o certificado em agosto de 2009.

2.3. Control Objectives for Information and Related Technology - COBIT

O COBIT é um framework que fornece as melhores práticas para o gerenciamento de processos de TI, estruturados de uma forma gerenciável e lógica, atendendo as várias necessidades de gestão da organização, tratando os riscos de negócio, questões técnicas, necessidades de controle e métricas de desempenho.

O desenvolvimento do COBIT foi iniciado em 1994 pela *Information Systems Audit and Control Foundation* – ISACF. A primeira publicação ocorreu em abril de 1996, enfocando o controle e análise de Sistemas de Informação. Em 1998 foi publicada a 2ª edição, que adicionou o guia prático de implantação e execução. A 3ª edição foi publicada em 2000 pelo *IT Governance Institute* – ITGI, órgão criado pela ISACA com o objetivo de promover um melhor entendimento e a adoção dos princípios de Governança de TI.

O modelo foi atualizado em dezembro de 2005 para a 4ª edição, com a revisão de práticas e padrões totalmente alinhados aos modelos COSO, ITIL e ISO/IEC 17799. Em maio de 2007 foi lançada a revisão 4.1 (a mais recente).

O COBIT procura ocupar o espaço entre a Gestão de Riscos voltada para o Negócio (atendida, por exemplo, pelo COSO – *Comitee of Sponsoring Organizations*), a Gestão de Serviços em TI (por exemplo, por meio do ITIL) e a Gestão da Segurança da Informação (por exemplo, tratada pela ISO/IEC 27001).

Esses modelos de gestão consistem de boas práticas específicas segundo sua área foco, e possuem funções complementares. Dessa forma, o COBIT permite alinhar os objetivos dessas áreas de conhecimento às estratégias e princípios de governança corporativa, garantindo, assim, que os processos e atividades desempenhadas pelas respectivas áreas e funções corporativas concorram de forma sistemática para o alcance os objetivos do negócio e para a redução dos riscos operacionais.

O COBIT ainda assegura aos usuários a existência de controles, inclusive tornando-os responsáveis por parte desses controles, e auxilia o trabalho dos auditores de sistemas e de segurança da informação.

O framework do COBIT fornece informações necessárias para suportar os objetivos de negócio e seus requisitos. O framework explica como os Processos de TI entregam informações que o negócio necessita para alcançar seus objetivos.

O princípio do framework é derivado de um modelo, conforme figura 2.3, que mostra a informação com qualidade sendo produzida por eventos através de recursos de TI.

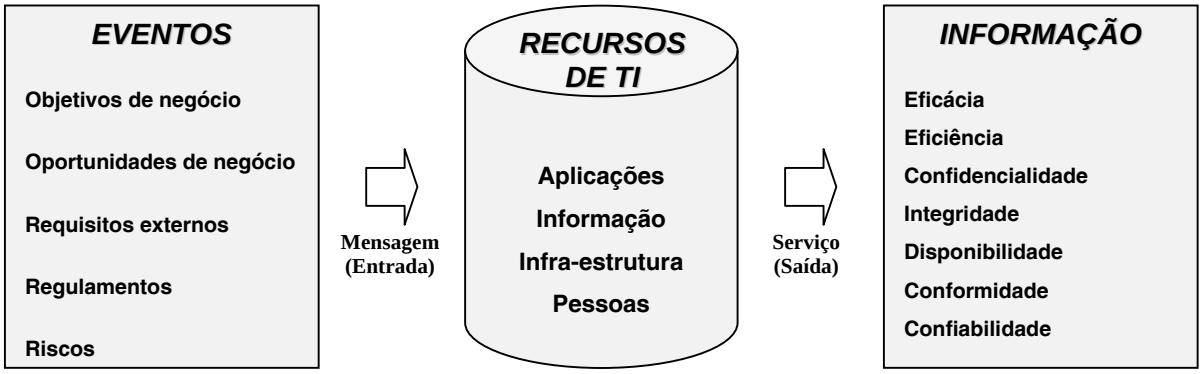

Figura 2.3 – Princípio do framework COBIT.

Fonte : IT Governance Institute, 2007a - adaptado

Conforme sugerido por Fernandes e Abreu (2006, p. 180), analisando o framework do COBIT de outra forma, podemos entendê-lo assim: os Recursos de TI são gerenciados por Processos de TI, para atingir Metas de TI, que por sua vez estão estreitamente ligadas aos Requisitos do Negócio.

Este é o princípio básico do framework COBIT, cujos três componentes formam as três dimensões do cubo do COBIT, conforme representado na figura 2.4, a seguir:

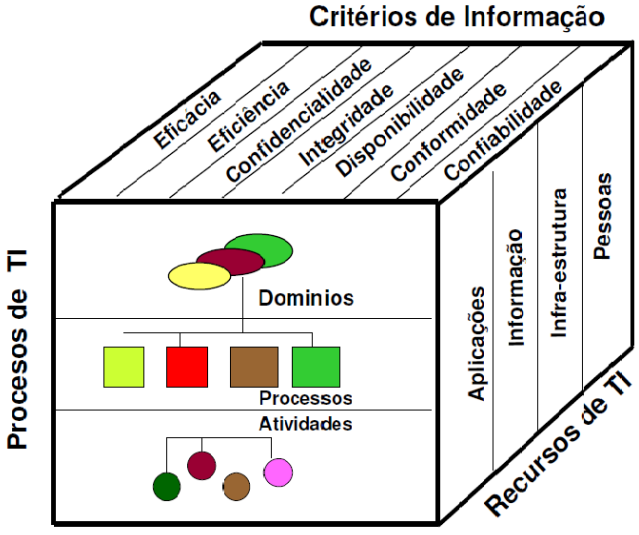

Figura 2.4 – Cubo COBIT.

Fonte: IT Governance Institute, 2007a - adaptado

O componente Processos de TI agrupa as principais atividades de TI em um modelo de processo, facilitando o gerenciamento dos recursos de TI para atender as necessidades do

negócio. Os processos de TI são definidos e classificados em 4 domínios sendo desmembrados e definidos em atividades e tarefas na organização.

Os domínios do COBIT são os seguintes:

- **Planejamento e Organização (PO[2])** – cobre o uso da tecnologia e o modo como esta pode ser melhor utilizada na organização para que os objetivos e metas sejam atingidos. Também destaca a organização e a forma como a infraestrutura de TI está preparada para otimizar resultados e gerar maiores benefícios do uso de TI;
- **Aquisição e Implementação (AI[3])** – Endereça a estratégia da empresa na identificação de requerimentos de TI, na aquisição de tecnologia e na implementação dentro dos processos de negócio;
- **Entrega e Suporte (DS[4])** – Foca nos aspectos da entrega da TI. Cobre áreas como execução de aplicações de sistemas de TI e seus resultados, bem como os processos de suporte que habilitam a execução desses sistemas com efetividade e eficiência. Os processos de suporte incluem objetivos de segurança e treinamento;e
- **Monitoramento e Avaliação (ME[5])** – Alinha com a estratégia da empresa, avaliando se as necessidades do negócio são atingidas com os sistemas de TI e se os objetivos de controle necessários cobrem os requerimentos regulatórios. Cobre também os objetivos de efetividade e disponibilidade, a auditoria e os objetivos de controles internos e externos.

O COBIT avalia o grau de confiança, qualidade e segurança adequados para as necessidades das corporações, provendo sete critérios de informação que podem ser empregados para definir genericamente o que os negócios requerem da TI: efetividade, eficiência, confidencialidade, integridade, disponibilidade, conformidade e confiabilidade.

A Figura 2.5 mostra o inter-relacionamento dos objetivos de negócio com a Governança de TI e esta com cada um dos domínios do COBIT, utilizando como matriz o ciclo tradicional de melhoria contínua (planejar, construir, executar e monitorar).

[2] A sigla “PO” vem do termo em inglês *Plan and Organize*
[3] A sigla “AI” vem do termo em inglês *Acquire and Implement*
[4] A sigla “DS” vem do termo em inglês *Deliver and Support*
[5] A sigla “ME” vem do termo em inglês *Monitor and Evaluate*

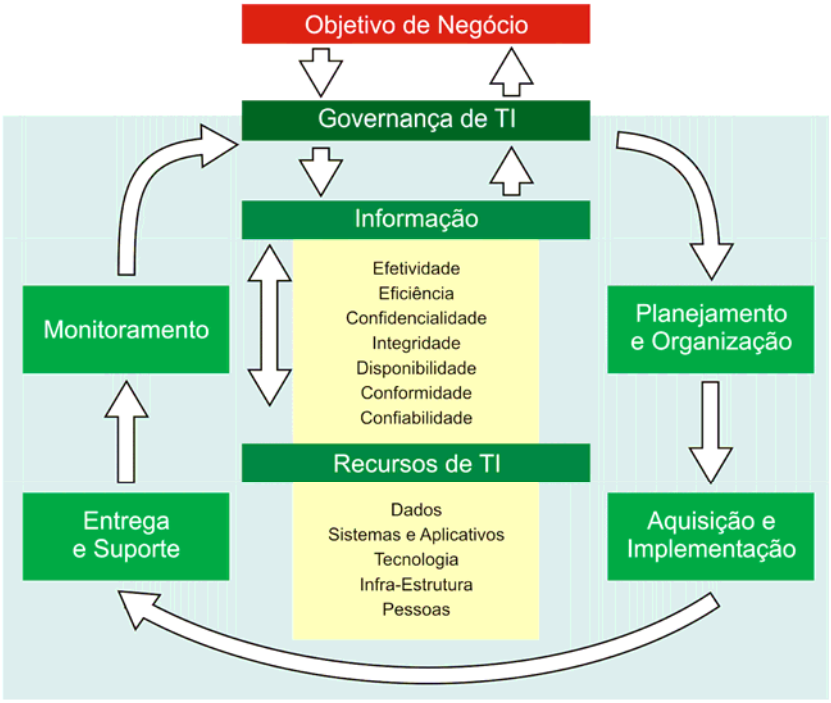

Figura 2.5 – Domínios do COBIT.

Fonte: IT Governance Institute, 2007a, p.26 - adaptado

Os quatro domínios estão subdivididos em 34 processos, que garantem a completude da gestão de TI, conforme descritos a seguir.

Domínio Planejamento e Organização (PO)

- **PO1 – Define a estratégia de TI:** clarifica e formaliza, por meio de um plano estratégico, até onde a organização pretende chegar, vinculando as diretrizes de TI às necessidades do negócio;
- **PO2 – Define a arquitetura da informação:** descreve como a organização dos Sistemas de Informação é suportada pela manutenção de um modelo de informações de negócio e pela garantia de que os sistemas são apropriados e estão definidos para otimizar o uso de informações;
- **PO3 – Determina a direção tecnológica:** visão de futuro de tecnologia e adesão à padrões;
- **PO4 – Define a organização de TI e seus relacionamentos:** estabelece a estrutura da área de TI, plano de carreira, cargos com seus papéis e os relacionamentos com as outras áreas da organização;

- **PO5 – Gerencia os investimentos de TI:** avalia o retorno dos investimentos, contabiliza o custeio e investimentos, e apropria por centro de custos;
- **PO6 – Gerencia a comunicação das diretrizes de TI:** desenvolve e implanta planos de comunicação que visam disseminar o conhecimento das estratégias de TI em toda a organização;
- **PO7 – Gerencia os recursos humanos:** cuida do recrutamento, contratação e capacitação da equipe em relação ao negócio e às tecnologias que compõem a diretriz tecnológica;
- **PO8 – Gerencia a qualidade:** observa a qualidade da entrega dos softwares e a utilização de modelos;
- **PO9 – Avalia e gerencia os riscos de TI:** analisa ameaças, impactos no negócio e vulnerabilidades da informação e das instalações, bem como a probabilidade de ocorrência; e
- **PO10 – Gerencia os projetos:** administra os projetos de TI observando modelos e melhores práticas de mercado.

Domínio Aquisição e Implementação (AI):

- **AI1 – Identifica soluções automatizadas**: analisa as necessidades de automação dos processos de negócio;
- **AI2 – Adquire e mantém software aplicativo**: define e aplica modelos de avaliação para a contratação de softwares;
- **AI3 – Adquire e mantém infraestrutura tecnológica**: define modelos de avaliação para contratação de equipamentos e serviços de infraestrutura;
- **AI4 – viabiliza operação e utilização**: cuida da construção de descrições formais dos processos da área de TI;
- **AI5 – Adquire recursos de TI**: cuida da instalação dos softwares em ambiente de homologação e dos testes de certificação que possibilitam a liberação para o ambiente de produção;
- **AI6 – Gerenciar mudanças**: cuida do gerenciamento formal e controlado das mudanças relativas a infraestrutura e as aplicações; e
- **AI7 – Instala e prova soluções e mudanças**: avalia e aprova mudanças no ambiente de TI, tanto em equipamentos e arquitetura como em sistemas e processos.

Domínio Entrega e Suporte (DS):

- **DS1 – Define e gerencia níveis de serviço**: formaliza os níveis de atendimento e solução requeridos pela área de TI dos seus fornecedores e das áreas de negócio em relação à área de TI;
- **DS2 – Gerencia serviços terceirizados**: acompanha e avalia os serviços contratados;
- **DS3 – Gerencia o desempenho e a capacidade**: define os recursos computacionais e garante que não haja escassez de recursos, nem tampouco subutilização, evitando problemas de desempenho nas aplicações ou desperdício de investimentos;
- **DS4 – Assegura a continuidade de serviços**: implanta arquiteturas computacionais de alta disponibilidade, que visam à manutenção dos sistemas e processos operacionais, reduzindo-se o impacto da indisponibilidade sobre o negócio;
- **DS5 – Assegura a segurança dos serviços**: visa à preservação da confidencialidade, da integridade e da disponibilidade, garantindo que somente pessoas autorizadas possam acessar a informação, à exatidão e à completeza da informação, e que, quando necessário, a informação estará disponível;
- **DS6 – Identifica e aloca custos**: aloca corretamente as despesas e investimentos de TI nos devidos centros de custos;
- **DS7 – Educa e treina os usuários**: cuida da definição e execução de uma estratégia efetiva de treinamento dos usuários e medição dos resultados;
- **DS8 – Gerencia a central de serviços e incidentes**: provê a rápida e efetiva resposta da TI às questões e incidentes relacionados aos usuários;
- **DS9 – Gerencia a configuração:** provê a manutenção do banco de dados de configuração de hardware e software;
- **DS10 – Gerencia os problemas**: provê a efetiva identificação, classificação, análise de causa raiz e resolução dos problemas;
- **DS11 – Gerencia os dados**: define o modelo de dados e o ciclo de vida da informação, especificando prazos para manutenção da informação de acordo com os requisitos do negócio e a legislação pertinente;
- **DS12 – Gerencia o ambiente físico**: administra, desenha e planeja, fornece suporte técnico, desenvolvimento e operação, focados nos desafios da infraestrutura de TI; e
- **DS13 – Gerencia as operações**: administra o funcionamento das operações de TI.

Domínio Monitoramento e Avaliação (ME):

- **ME1 – Monitora e avalia o desempenho da TI**: cuida da definição dos indicadores de desempenho, da avaliação e atua nas situações de desvio;
- **ME2 – Monitora e avalia os controles internos**: estabelece um programa efetivo de controle interno, responsável por monitorar as situações de exceção quanto aos controles estabelecidos;
- **ME3 – Assegura conformidade com as regulações**: estabelece um processo de revisão para garantir a conformidade com as leis, regulamentos e requisitos contratuais; e
- **ME4 – Fornece governança para a TI**: cuida da definição de estruturas organizacionais, processos, papéis e responsabilidades para garantir que os investimentos da TI estão alinhados com as estratégias e objetivos da organização.

Os processos do COBIT podem ser aplicados em vários níveis na organização, de tal forma que alguns destes processos podem ser aplicados a nível corporativo, outros ao nível de função de TI, e os demais no nível do responsável pelo processo de negócio.

Para satisfazer os objetivos de negócio, as informações precisam estar em conformidade com um critério específico. No COBIT estes critérios são chamados de requisitos de negócio para informação. Para estabelecer a lista de requisitos, o COBIT combina os princípios embutidos nos modelos de referências existentes e conhecidos. Estes três requisitos são: Requisitos de Qualidade, Requisitos de Segurança e Requisitos Fiduciários.

Os três requisitos – Qualidade, Segurança e Fiduciário – são divididos em sete categorias distintas que podem se sobrepor:

- **Eficácia**: é a capacidade de alçar metas e resultados propostos. Trata da informação que está sendo relevante e pertinente ao processo de negócio, bem como que esteja sendo entregue de um modo oportuno, correto, consistente e útil;
- **Eficiência**: capacidade de produzir o máximo nos resultados com o mínimo de recursos. Diz respeito à provisão da informação através do uso otimizado (mais produtivo e econômico) dos recursos. Tem foco na otimização de custos;

- **Confiabilidade**: relaciona-se à provisão de informação apropriada para a gerência operar a entidade e para a gerência exercer suas responsabilidades de relatar aspectos de conformidade e finanças;
- **Conformidade**: trata do cumprimento das leis, dos regulamentos e arranjos contratuais aos quais o processo de negócio está sujeito;
- **Confidencialidade**: diz respeito à proteção da informação sigilosa contra a revelação não autorizada;
- **Integridade**: relaciona-se à exatidão e à inteireza da informação bem como à sua validez de acordo com os valores e expectativas do negócio; e
- **Disponibilidade**: relaciona-se à informação que está sendo disponibilizada quando requerida pelo processo de negócio agora e no futuro. Também diz respeito à salvaguarda dos recursos necessários e às capacidades associadas.

As medidas de controle para cada processo de TI, e por sua vez do COBIT, não satisfazem todos os requisitos de negócio no mesmo grau. O framework do COBIT define três graus de controle da informação:

1. **Primário**: impacta diretamente o critério de informação a que se refere;
2. **Secundário**: satisfaz parcialmente ou indiretamente o critério de informação a que se refere; e
3. **Em Branco:** pode ser aplicável; entretanto, os requisitos são satisfeitos de forma mais apropriada por outro critério neste processo e/ou ainda por outro processo.

A figura 2.6 fornece uma indicação por processo de TI e domínio, informando qual critério de informação é impactado e em qual medida (P = Primário, S = Secundário) por um objetivo controle de alto nível e quais recursos de TI são aplicáveis (aplicações, informações, infraestrutura e pessoas).

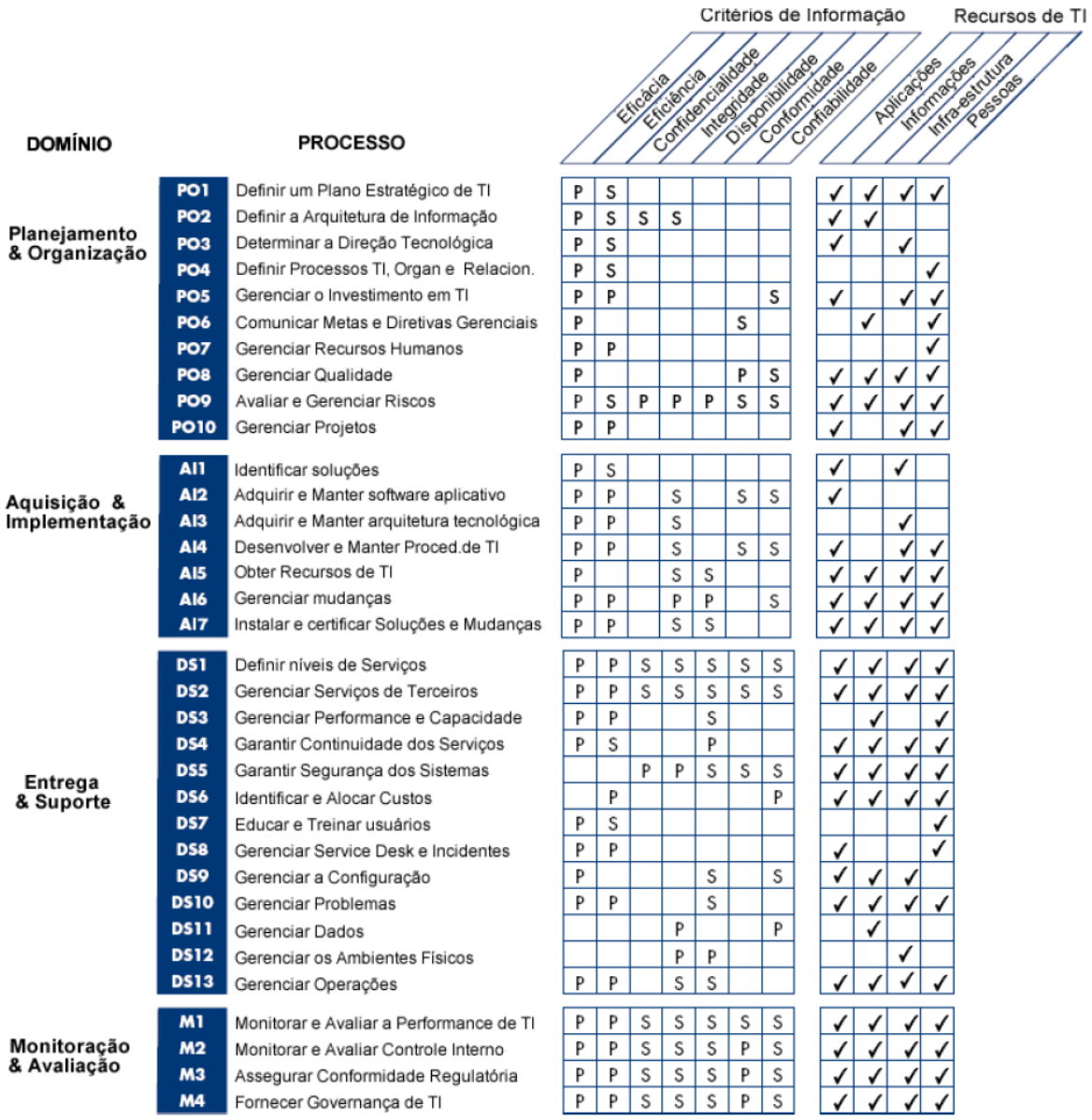

Figura 2.6 – Relação de impacto e aplicabilidade (objetivo de controle versus critérios de informação e recursos de TI). Fonte: IT Governance Institute, 2007a - adaptado

Para cada processo do COBIT, as atividades chaves são definidas junto com um gráfico RACI que serve para definir as tarefas que precisam ser delegadas (atividades) e para quem (funções), de acordo com os seguintes papéis:

- **Responsável (Responsible):** é a pessoa que executa a atividade;
- **Aprovador (Accountable**): é a pessoa que fornece direção e autoriza uma atividade. Esta função não pode ser delegada;
- **Consultado (Consulted):** é qualquer pessoa que suporte a atividade; e
- **Informado (Informed):** é qualquer pessoa que esteja envolvida com a atividade.

Atividades \ Funções	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Associar os objetivos do negócio aos objetivos de TI.	C	I	A/R	R	C						
Identificar dependências críticas e a performance atual.	C	C	R	A/R	C	C	C	C	C		C
Construir um plano estratégico de TI.	A	C	C	R	I	C	C	C	C	I	C
Construir planos táticos de TI.	C	I		A	C	C	C	C	C	R	I
Analisar os portfólios de programa e gerenciar projetos e portfólios de serviço.	C	I	I	A	R	R	C	R	C	C	I

Figura 2.7 – Gráfico RACI do Processo PO1 - Define a estratégia de TI.

Fonte: IT Governance Institute, 2007a, p. 31 - adaptado

Segundo Fernandes e Abreu (2006, p. 183) entre as várias oportunidades de aplicação em uma organização, devido a grande abrangência e o alto grau de padronização, o CobiT é utilizado para avaliar os processos de TI, servindo como checklist para avaliar os pontos fortes e os pontos fracos dos seus processos, servindo como subsídio para a proposição de ações de melhoria.

Nesta pesquisa, que trata da avaliação de maturidade de processos de TI do Superior Tribunal de Justiça, focaremos no processo DS4, do domínio *Deliver and Support* (Entrega e Suporte), que trata da garantia de continuidade dos serviços. Analisaremos em profundidade a estrutura deste processo, conhecendo seus objetivos de controle, as atividades e funções necessários a sua efetividade (gráfico RACI) e o modelo de maturidade definido.

2.4. Processo DS4 do COBIT

Um dos processos de TI identificado no framework é o DS4 Garantir Continuidade dos Serviços, do domínio *Deliver and Support*, que indica melhores práticas para garantia da continuidade de serviços.

A necessidade de prover serviços de TI de forma contínua requer o desenvolvimento, manutenção e testes do Plano de Continuidade de TI, utilizando-se armazenamento externo de backup e realizando-se periodicamente treinamento sobre o plano de continuidade. A efetividade do processo de serviço contínuo minimiza a probabilidade e o impacto de

interrupções prolongadas dos serviços de TI nos processos e funções chave do negócio (IT Governance Institute, 2007, p. 113).

Ainda segundo o IT Governance Institute, o controle sobre o processo de garantir a continuidade dos serviços satisfaz o requisito de negócio que estabelece o dever da TI garantir o mínimo impacto no negócio na ocorrência de um evento de interrupção no serviço, focando sua atenção na implementação de resiliência nas soluções automatizadas e desenvolvendo, mantendo e testando planos de continuidade de TI. Este objetivo é alcançado com a execução das seguintes atividades:

- Desenvolvimento e manutenção (aperfeiçoamento) dos mecanismos de contingência de TI;
- Realização de treinamento e testes nos planos de contingência de TI; e
- Armazenamento de cópias dos planos de contingências e dos dados em instalações externas.

A efetividade do processo de garantir a continuidade dos serviços é avaliada a partir das seguintes métricas:

- Número de horas perdidas por usuário, apuradas mensalmente, motivadas por paradas não programadas; e
- Número de processos críticos de negócio suportados pela área de TI, não abrangidos pelo plano de continuidade.

As medidas de controle definidas no processo DS4, atendem a três critérios de controle da informação:

- **Eficácia**: atendido de forma Primária (P);
- **Eficiência**: atendido de forma secundária (S); e
- **Disponibilidade**: atendido de forma Primária (P).

O processo DS4, encarregado de garantir a continuidade dos serviços, similar ao que ocorre com os demais processos, possui papéis e responsabilidades definidos sem ambigüidades, estabelecidos de acordo com o gráfico RACI mostrado na figura 2.8.

Atividades \ Funções	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Desenvolver um framework de continuidade de TI		C	C	A	C	R	R	R	C	C	R
Conduzir análise de impacto nos negócios e avaliações de risco		C	C	C	C	A/R	C	C	C	C	C
Desenvolver e manter planos de continuidade de TI	I	C	C	C	I	A/R		C	C	C	C
Identificar e categorisar os recursos de TI baseado nos objetivos de recuperação				C		A/R		C	I	C	I
Definir e executar procedimentos de controle de mudanças para assegurar que o plano de continuidade de TI está atualizado				I		A/R		R	R	R	I
Testar regularmente o plano de continuidade de TI				I	I	A/R		C	C	I	I
Desenvolver um plano de acompanhamento a partir do resultado do teste				C	I	A/R	C	R	R	R	I
Planejar e conduzir treinamento em continuidade de TI				I	R	A/R		C	R	I	I
Planejar a recuperação dos serviços de TI e a retomada		I	I	C	C	A/R	C	R	R	R	C
Planejar e implementar o armazenamento e a proteção do backup				I		A/R		C	C	I	I
Estabelecer procedimentos para conduzir revisões pós-retomada				C	I	A/R		C	C		C

Figura 2.8 – Gráfico RACI do Processo DS4 - Garantir a Continuidade do Serviço.

Fonte: IT Governance Institute, 2007a, p. 115 - adaptado

Analisando as informações do gráfico RACI, é possível perceber que relativo ao processo DS4, a função de Head Operations (Líder das Operações de TI) é o responsável por executar todas as 11 atividades definidas, sendo em várias delas o único executor.

Com relação aos objetivos de controle do processo DS4, são 10 objetivos de controle que definem o resultado desejado ou propósito a ser atingido por meio da implantação de procedimentos de controle. O detalhamento dos objetivos de controle do processo DS4 será abordado no capítulo 5.

Segundo Fernandes e Abreu (2006, p. 179) um dos maiores desafios das organizações é visualizar o nível de profundidade que deve ser adotado pelos mecanismos de controle e medições de desempenho.

O COBIT fornece para os 34 processos de TI, diretrizes contendo ferramentas de avaliação e medição do ambiente de TI da organização. Uma das abordagens utilizadas para avaliação gerencial do estágio de evolução da implantação do modelo é o *IT Governance Maturity Model*, que será explorado a seguir.

2.5. IT Governance Maturity Model

Os modelos de maturidade de governança são usados para o controle dos processos de TI e fornecem um método eficiente para classificar o estágio da organização de TI.

Essa abordagem é derivada do modelo de maturidade para desenvolvimento de software, Capability Maturity Model for Software (SW-CMM), proposto pelo Software Engineering Institute (SEI), definido para a maturidade da capacidade de desenvolvimento de software. Embora os conceitos da abordagem SEI tenham sido seguidos, a implementação do COBIT difere consideravelmente do SEI original, que foi orientada sobre princípios aplicáveis à produtos de engenharia de software, à organizações que disputam a excelência nestas áreas e a avaliação formal dos níveis de maturidade para que os desenvolvedores de software possam ser certificados.

No COBIT, uma definição genérica é fornecida para a escala de maturidade, que é semelhante ao CMM, mas interpretado pela natureza dos processos de gerenciamento de TI. Um modelo específico é fornecido a partir desta escala genérica para cada um dos 34 processos do COBIT. Seja qual for o modelo, COBIT ou CMM, as escalas não são muito granulares, fato que tornaria os sistemas difíceis de usar e sugeririam uma precisão injustificada dado que, em geral, o objetivo de se avaliar a maturidade é identificar quais são os pontos a serem tratados e definir as prioridades das melhorias, ou seja, o objetivo não é avaliar o nível de adesão aos objetivos de controle.

Os níveis de maturidade são concebidos como perfis dos processos de TI que uma organização deva reconhecer como descrições de possíveis estados atuais e futuros. Eles não são projetados para uso como um modelo de limiar, onde não pode se mover para o próximo nível superior sem ter cumprido todas as condições de nível inferior. No modelo de maturidade do COBIT, ao contrário da abordagem original do SEI/CMM, não há intenção de medir os níveis de precisão ou tentar certificar que o nível foi exatamente cumprido. Na avaliação de maturidade do COBIT é provável que o resultado aponte um perfil em que as condições relevantes para diversos níveis de maturidade foram cumpridas, como mostrado no gráfico de exemplo na figura 2.9. (IT Governance Institute, 2007a, p. 18)

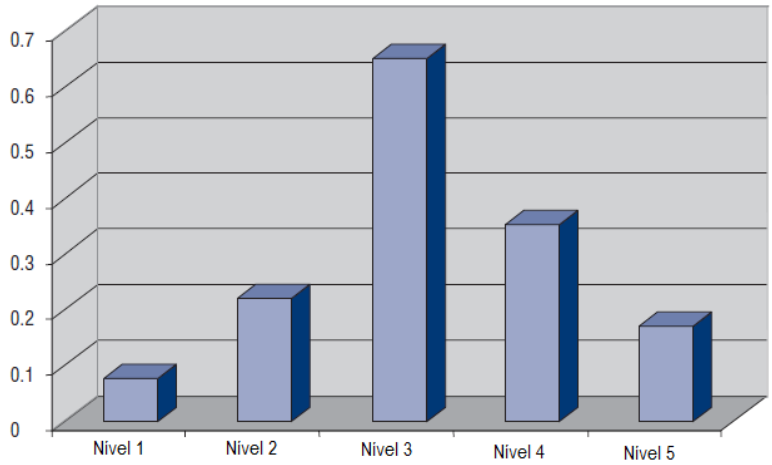

Figura 2.9 – Possível nível de maturidade de um processo de TI: O exemplo ilustra um processo que está praticamente no nível 3, mas ainda tem algumas questões de conformidade com os requisitos de nível inferior, enquanto que já investe em medição de desempenho (nível 4) e otimização (nível 5).
Fonte: IT Governance Institute, 2007a, p. 18 - adaptado

O modelo de maturidade genérico da Governança de TI descreve os processos e atividades, requeridos em cada um dos seis níveis de maturidade, a saber (IT Governance Institute, 2003, p. 48):

- **0 – Inexistente**: não há gerenciamento de atividades relacionadas a TI para medir o que os objetivos de TI adicionam de valor para a organização, nem para medir se os riscos relacionados com TI são apropriadamente gerenciados;
- **1 – Inicial / Ad hoc**: O conceito de Governança de TI não existe formalmente e a supervisão se baseia principalmente em considerações gerenciais de objetivos relacionados de TI, analisados caso a caso. A Governança de TI depende da iniciativa e da experiência de um time de gerenciamento, que limita a entrada dos demais integrantes da organização. A alta gerência somente é envolvida quando surgem problemas mais graves. O gerenciamento de desempenho é tipicamente limitado a medidas técnicas, e somente dentro de funções de TI;
- **2 – Repetitivo, mas intuitivo**: A realização supera a formalização. Requer supervisão de TI, sendo necessário compartilhar responsabilidades com a gerência sênior. Práticas regulares de Governança são metas. A criação de relatórios regulares de desempenho e investigação de problemas tomou lugar recentemente nas iniciativas do time de TI. Usuários-chave ou stakeholders são participantes voluntários ou cooptados, dependendo do projeto de TI e das prioridades;

- **3 – Processos definidos**: Um framework organizacional e de processos está definido para a supervisão e gerenciamento de atividades de TI e está sendo introduzido na organização como base para Governança de TI. O corpo gerencial tem objetivos de direção, que têm sido desenvolvidos segundo procedimentos específicos de gerenciamento, compatíveis com atividades de Governança. Isso inclui: ajuste regular de objetivos, revisão de desempenho, assessments de capacidade necessária e planejamento de projetos e recursos para qualquer necessidade de implementação de TI. Práticas informais prévias bem sucedidas foram formalizadas, e as técnicas seguidas são relativamente simples e não sofisticadas;
- **4 – Processos gerenciáveis e medidos**: Ajustes de objetivos foram desenvolvidos para um estágio sofisticado, com relacionamentos entre objetivos externos em termos de negócios. Processos de TI provêem métricas bem compreendidas. Resultados reais são comunicados à alta gerência na forma de Balanced Scorecard. O time da gerência corporativa agora trabalha junto com os objetivos de maximizar o valor da entrega de serviços de TI e gerenciar os riscos relacionados à TI. Existe um assessment regular das capacidades de TI e os projetos têm sido entregues com os requisitos reais de desempenho. Relacionamentos entre as funções de TI, seus usuários da comunidade de negócios e provedores externos são agora baseados em funções definidas e acordos de níveis de serviço; e
- **5 – Processos otimizados**: Práticas de Governança de TI são desenvolvidas segundo uma sofisticada abordagem, empregando técnicas eficazes. Existe uma verdadeira transparência das atividades de TI e o corpo diretivo percebe o controle das estratégias de TI. Atividades de TI são priorizadas de acordo com a real prioridade do negócio, o valor entregue para a corporação pode ser medido e passos adotados tempestivamente corrigem desvios significativos ou problemas. A abordagem do Balanced Scorecard evoluiu, tornando-se a mais relevante medida de estratégia de negócios corporativos. O esforço despendido no gerenciamento de risco é minimizado por meio da adoção de padrões e automação de processos. A prática de melhoria contínua da capacidade de TI está embebida na cultura, incluindo benchmarking. Auditorias independentes provêem garantias de gerenciamento. Além disso, o custo de TI é efetivamente monitorado, e a organização está habilitada para melhorar continuamente. Seletivamente, serviços

foram terceirizados. A organização está habilitada para demonstrar excelência de desempenho e demandar melhores práticas de outras organizações.

A gestão do processo DS4 – Garantir a Continuidade do Serviço é avaliada quanto a sua maturidade de acordo com os seguintes critérios (IT Governance Institute, 2007a, p. 116):

- **DS4 – Nível 0 (Inexistente)**: quando não há a compreensão dos riscos, vulnerabilidades e ameaças para as operações de TI ou o impacto da perda de serviços de TI para o negócio. A continuidade de serviço não é considerada necessária pela administração;
- **DS4 – Nível 1 (Inicial/Ad hoc)**: quando as responsabilidades pela continuidade de serviços são informais, e a autoridade para executar as responsabilidades é limitada. A administração torna-se consciente dos riscos relacionados e percebe a necessidade da continuidade de serviço. O foco de atenção da gestão da continuidade de serviço é sobre os recursos de infraestrutura, em vez dos serviços de TI. Os usuários implementam soluções alternativas em resposta às interrupções do serviço. A resposta da TI para paradas significativas é reativa e não-planejada. Interrupções planejadas são agendadas para atender necessidades da TI, mas não consideram os requisitos de negócio;
- **DS4 – Nível 2 (Repetitivo, mas intuitivo**): quando a responsabilidade de assegurar a continuidade do serviço é permanente e é formalmente atribuída. As estratégias para assegurar a continuidade do serviço são fragmentadas. Relatórios sobre a disponibilidade dos sistemas são esporádicos, podendo estar incompletos e não levarem em conta o impacto nos negócios. Não há nenhum plano de continuidade de TI documentado, embora haja compromisso com a disponibilidade contínua do serviço e os seus princípios mais importantes são conhecidos. Existe um inventário dos sistemas e componentes críticos, mas pode não ser confiável. Práticas de serviços contínuos estão em fase inicial, mas o sucesso depende de pessoas;
- **DS4 – Nível 3 (Definido)**: quando a prestação de contas pela gestão da continuidade é inequívoca. As responsabilidades pelo planejamento e testes da continuidade dos serviços são claramente definidas e caracterizadas. O plano de continuidade de TI está documentado e é baseado na criticidade dos sistemas e no

respectivo impacto nos negócios. Há apresentação periódica de relatórios de testes da continuidade dos serviços. A equipe toma a iniciativa de seguir as normas e recebe treinamento para lidar com incidentes significativos ou desastres. A equipe de gestão comunica, de forma consistente, a necessidade do plano para assegurar a continuidade do serviço. São empregados componentes que permitem a alta disponibilidade e redundância dos sistemas. O inventário dos sistemas e componentes críticos é mantido atualizado;

- **DS4 – Nível 4 (Gerenciado e Medido)**: Quando as responsabilidades e normas da continuidade do serviço são aplicadas. A responsabilidade de manter o plano de continuidade do serviço contínuo é formalmente atribuída. As atividades de manutenção do plano são baseadas nos resultados dos testes, nas boas práticas internas, e na evolução dos ambiente de TI e de negócios. Dados sobre a continuidade dos serviços estão sendo coletados, analisados e comunicados, gerando ações de correção. É obrigatória a participação em treinamento formal sobre os processos de continuidade do serviço. Boas práticas de disponibilidade de sistemas estão sendo implantadas de forma consistente. As atividades de implementação de disponibilidade influenciam o planejamento da continuidade dos serviços e vice-versa. Os incidentes de descontinuidade são classificados, sendo conhecida por todos os envolvidos a escala de classificação. Objetivos e métricas para a continuidade do serviço foram desenvolvidos e acordados, mas pode ser medidos de forma inconsistente; e
- **DS4 – Nível 5 (Otimizado)**: quando os processos de continuidade do serviço funcionam de forma integrada, levando em conta benchmarking e melhores práticas externas. O plano de continuidade de TI é integrado com os planos de continuidade de negócios e são atualizados periodicamente. Os requisitos para assegurar o serviço permanente são garantidos pelos principais fornecedores. Ocorrem testes globais do plano de continuidade de TI, e os resultados dos testes são as entradas para o processo de atualização do plano. A coleta e análise dos dados são utilizadas na melhoria contínua do processo. As práticas de disponibilidade e o planejamento da continuidade dos serviços estão perfeitamente alinhados. A gestão do processo de continuidade assegura que uma catástrofe ou incidente grave não irá ocorrer como resultado de um único ponto de falha. As práticas de escalação de incidentes são entendidas e bem executadas. Objetivos e

métricas sobre a eficiência da continuidade dos serviços são medidos de forma sistemática. A equipe de gestão ajusta o planejamento da continuidade dos serviços de forma contínua em resposta as métricas avaliadas.

2.6. Alinhamento dos Objetivos de Controle do COBIT 4.1 e da ISO/IEC 27001:2005 para o Processo de Continuidade dos Serviços de TI

> As melhores práticas de TI precisam estar alinhadas aos requisitos do negócio e integradas entre si e com os procedimentos internos da organização. O COBIT pode ser usado no nível mais alto, provendo um framework global de controle baseado em um modelo de processo de TI que podem atender todas as organizações, de uma forma genérica. Práticas e normas específicas, tais como as definidas na ISO/IEC 27001 abrangem áreas distintas e podem ser mapeados para a estrutura do COBIT, proporcionando assim uma hierarquia de orientação de tais práticas. (ITGI 2008, p. 22).

O quadro abaixo demonstra o relacionamento dos objetivos de controle do COBIT e da ISO/IEC 27002, considerando especificamente o processo DS4.

DS4 – GARANTIR A CONTINUIDADE DOS SERVIÇOS		
A necessidade de prover serviços de TI de forma contínua requer o desenvolvimento, manutenção e testes do Plano de Continuidade de TI, utilizando-se armazenamento externo de backup e realizando-se periodicamente treinamento sobre o plano de continuidade. A efetividade do processo de serviço contínuo minimiza a probabilidade e o impacto de interrupções prolongadas dos serviços de TI nos processos e funções chave do negócio.		
Objetivo de Controle COBIT 4.1	**Área Chave**	**Objetivo de Controle ISO/IEC 27002**
DS4.1 – Framework de Continuidade de TI	• Abordagem consistente de toda a organização para o gerenciamento da continuidade	• 6.1.6 - Contact with authorities • 6.1.7 - Contact with special interest groups • 14.1.1 - Including information security in the business continuity management process • 14.1.2 - Business continuity and risk assessment • 14.1.4 - Business continuity planning framework
DS4.2 – Planos de Continuidade de TI	• Planos de continuidade individuais baseados no framework • Análise de impacto no negócio • Resiliência, processamento alternativo e recuperação	• 6.1.6 - Contact with authorities • 6.1.7 - Contact with special interest groups • 14.1.3 - Developing and implementing continuity plans including information security
DS4.3 – Ativos críticos de TI	• Foco na infraestrutura crítica, resiliência e priorização • Resposta a diferentes períodos de tempo	• 14.1.1 - Including information security in the business continuity management process • 14.1.2 - Business continuity and risk assessment

DS4.4 – Manutenção do plano de continuidade de TI	• Controle de mudanças para refletir as mudanças nos requisitos do negócio	• 14.1.5 - Testing, maintaining and reassessing business continuity plans
DS4.5 – Testar o plano de continuidade de TI	• Testes regulares • Implementar o plano de ação	• 14.1.5 - Testing, maintaining and reassessing business continuity plans
DS4.6 – Treinamento no plano de continuidade de TI	• Treinar regularmente todos os interessados	• 14.1.5 - Testing, maintaining and reassessing business continuity plans
DS4.7 – Distribuição do plano de continuidade de TI	• Distribuição adequada e segura a todos os interessados	• 14.1.5 - Testing, maintaining and reassessing business continuity plans
DS4.8 – Retomando e recuperando os serviços de TI	• Planejamento para o período quando a TI está recuperando e retomando os serviços • Conhecimento do negócio e de apoio ao investimento	• 14.1.1 - Including information security in the business continuity management process • 14.1.3 - Maintain or restore operations and ensure availability of information
DS4.9 – Armazenamento do Backup Offsite	• Armazenamento externo de todas as mídias críticas, a documentação e os recursos necessários, em colaboração com os proprietários de processos de negócios	• 10.5.1 - Information backup
DS4.10 – Revisão pós-retomada	• Avaliação periódica dos planos	• 14.1.5 - Testing, maintaining and reassessing business continuity plans

Figura 2.10 – Alinhamento dos objetivos de controle do COBIT 4.1 e da ISO/IEC 27002.

Fonte: IT Governance Institute, 2008 - adaptado

3. CENÁRIO, LEGISLAÇÃO E METODOLOGIAS APLICADAS AO PROCESSO JUDICIAL ELETRÔNICO NO ÂMBITO DO STJ

3.1. Cenário – Composição do Poder Judiciário Brasileiro e Atribuições do STJ

A Constituição da República Federativa do Brasil de 1988 define, em seu artigo 92, a composição do Poder Judiciário, da seguinte forma:

- I – o Supremo Tribunal Federal;
- I-A – o Conselho Nacional de Justiça;
- II – o Superior Tribunal de Justiça;
- III – os Tribunais Regionais Federais e os Juízes Federais;
- IV – os Tribunais e os Juízes do Trabalho;
- V – os Tribunais e os Juízes Eleitorais;
- VI – os Tribunais e os Juízes Militares; e
- VII – os Tribunais e os Juízes dos Estados e do Distrito Federal e Territórios.

Dentre os órgãos acima relacionados, apenas o Conselho Nacional de Justiça não tem função jurisdicional, sendo de sua alçada o controle da atuação administrativa e financeira do Poder Judiciário e do cumprimento dos deveres funcionais dos juízes. Todos os demais exercem a função jurisdicional, e estão organizados em uma estrutura hierárquica.

O Artigo 105 da Constituição define a competência do STJ. Em seu inciso I, define as matérias que devem ser processadas e julgadas originariamente, e em seus incisos II e III define as matérias cujos recursos devem ser julgados no STJ. Nos últimos dois casos, são julgados pelo STJ apenas causas que tenham sido decididas pelos Tribunais Regionais Federais ou pelos tribunais dos Estados, do Distrito Federal e Territórios, sendo excluídas as causas de competência das justiças especializadas (Trabalhista, Eleitoral e Militar).

O Artigo 101, por sua vez, define a competência do Supremo Tribunal Federal, incluindo o processamento e julgamento de conflitos de competência entre o Superior Tribunal de Justiça e quaisquer tribunais, bem como “habeas-corpus”, mandado de segurança,

"habeas-data" e mandado de injunção, se decididos em única instância pelos Tribunais Superiores e sendo denegatória a decisão.

Em termos de fluxo processual, portanto, o STJ se posiciona dentro do Poder Judiciário Brasileiro conforme indicado na figura 3.1:

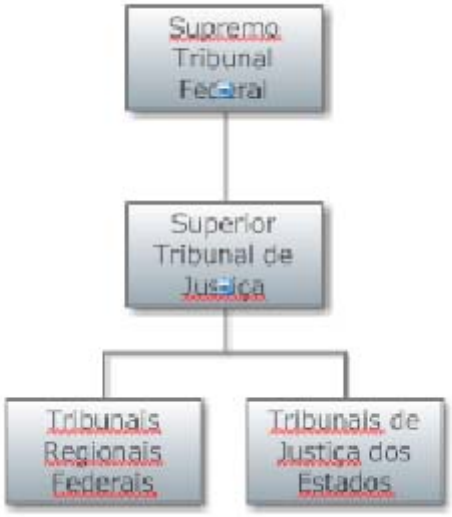

Figura 3.1 – Hierarquia simplicada do Poder Judiciário brasileiro.

3.2. A Evolução da Legislação e o Processo Judicial Eletrônico.

A morosidade do Poder Judiciário brasileiro tem sido constantemente apontada pela sociedade como um dos sérios problemas que o Brasil deve enfrentar, uma vez que o acesso democrático é ágil à justiça e é condição básica para a dignidade humana, conceito este encontrado inclusive na Constituição brasileira. Com efeito, Flávia Piovesan (1996, p. 63/64) em seu livro "Direitos Humanos e o Direito Constitucional Internacional", nos diz o seguinte:

> *"... atente-se ainda que, no intuito de reforçar a imperatividade das normas que traduzem direitos e garantias fundamentais, a Constituição de 1988 institui o princípio da aplicabilidade imediata dessas normas, nos termos do art. 5º, parágrafo 1º. Este princípio realça a força normativa de todos os preceitos constitucionais referentes a direitos, liberdades e garantias fundamentais, prevendo um regime jurídico específico endereçado a estes direitos. Vale dizer, cabe aos Poderes Públicos conferir eficácia máxima e*

> *imediata a todo e qualquer preceito definidor de direito e garantia fundamental".*

Diversas são as causas desta morosidade observada na prestação jurisdicional. Além daquelas relacionadas à estrutura do Poder Judiciário brasileiro, tais como estrutura insuficiente de fóruns, serventuários e juízes, bem como fatores conjunturais, tais como o excesso de demanda provocada por ações governamentais, há aquelas intrinsecamente ligadas à natureza do processo judicial em si, tanto no tocante à prática de atos processuais como com relação ao seu trâmite.

> *O processo judicial consiste na tentativa de traduzir em documentos (autos) um ou mais fatos que ocorreram na vida real, para o julgamento por terceiro (juiz) que não presenciou estes atos. Isto sempre demandará tempo razoável. A preocupação com a morosidade da justiça não é apenas um problema nacional. Vários países têm procurado resolver, ou pelo menos atenuar o problema, reformando leis e procedimentos. (PEDROSA, 2003)*

Diversas iniciativas vêm sendo tomadas no intuito de solucionar o problema em tela, desde medidas relacionadas à esfera jurídica, tais como a edição de Súmulas Vinculantes, que visam diminuir a quantidade de processos e

ncaminhados às instâncias superiores, passando por medidas estruturais, tais como a instituição de Juizados Especiais, destinados a promover a conciliação, o julgamento e a execução das causas consideradas de menor complexidade pela legislação, e alcançando medidas que visam agilizar o trâmite processual em si.

Trazendo o foco para este último conjunto de medidas, podemos observar uma crescente preocupação das autoridades pela adoção daquelas que pudessem agilizar o trâmite processual por meio da aplicação de soluções de tecnologia. Tal preocupação fica evidenciada através da observação da evolução legislativa relacionada ao assunto:

- Lei 9.800/1999 - Permitiu às partes a utilização de sistema de transmissão de dados para a prática de atos processuais;
- MPV n 2.200-2/2001 - Instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP-BRASIL e conferiu validade jurídica a documentos em forma eletrônica;
- Lei 11.280/2006 – Alterou diversos artigos do Código de Processo Civil, inclusive no que se refere à forma dos atos processuais, admitindo o meio eletrônico; e

- Lei 11.419/2006 – Dispôs sobre a informatização do Processo Judicial.

Como se vê, a aceitação de soluções tecnológicas no âmbito do Processo Judicial vem evoluindo desde 1999, quando primeiramente foi regulamentada a transmissão de dados para a prática de atos processuais, sendo exigida, entretanto, a entrega posterior dos documentos originais, até a viabilização do Processo Judicial Eletrônico, por meio da Lei 11.419/2006.

3.3. Lei 11.419/06

A Lei 11.419/06, de 19 de dezembro de 2006, admite o uso de meio eletrônico na composição de processos judiciais e é aplicável, indistintamente, aos processos civil, criminal e trabalhista, bem como aos juizados especiais, em qualquer grau de jurisdição.

A lei é dividida em três capítulos, a saber:

- Capítulo I - Informatização do processo judicial, que dentre outras providências, define como meio eletrônico *"qualquer forma de armazenamento ou tráfego de arquivos digitais"*;
- Capítulo II - Comunicação Eletrônica dos Atos Processuais, que possibilita a criação de Diário de Justiça Eletrônico;
- Capítulo III - Processo Eletrônico, que diz que *"Os órgãos do Poder Judiciário poderão desenvolver sistemas eletrônicos de processamento de ações judiciais por meio de autos total ou parcialmente digitais, utilizando, preferencialmente, a rede mundial de computadores e acesso por meio de redes internas e externas."*

O capítulo I, portanto, nos oferece uma definição de meio eletrônico que engloba a utilização de recursos computacionais, visto que atualmente são a tecnologia utilizada como suporte a arquivos digitais.

Já os capítulos II e III permitem a substituição do suporte físico tradicional, o papel, pelo suporte baseado em recursos computacionais, tanto do Diário de Justiça, originalmente impresso e distribuído pela Imprensa Nacional, quando do Processo Judicial em si.

Diversos benefícios podem ser alcançados a partir da adoção do meio eletrônico como suporte para o Processo Judicial, dentre os quais podemos destacar os seguintes:

- Universalização do acesso aos autos processuais, que deixa de requerer a presença física do interessado nas dependências do órgão onde o processo estiver armazenado, e passa a ser possível a qualquer parte interessada, e devidamente autorizada, a partir de qualquer dispositivo conectado à rede mundial de computadores;
- Maior agilidade na composição do Processo em si, uma vez que os documentos produzidos pelos órgãos do Poder Judiciário já podem ser elaborados a partir do próprio sistema de informática desenvolvido para materializar o processo, prescindindo de atividades manuais tais como a perfuração de folhas, aplicação de carimbos, etc, e os documentos apresentados pelos Advogados e partes interessadas podem ser enviados ao órgão, e eletronicamente inseridos no processo, por meio de páginas disponibilizadas nos sítios destes órgãos existentes na rede mundial de computadores;
- Maior agilidade no trâmite do processo, tanto internamente, entre unidades do órgão em que o mesmo estiver armazenado, quanto externamente, quando do envio do processo para a instância inferior ou superior, uma vez que a necessidade de movimentação física do processo em papel é substituída por sua transmissão eletrônica através de redes de computadores;
- Diminuição do impacto ambiental das atividades referentes à prestação jurisdicional, em função da diminuição do consumo de papel, bem como do consumo de combustíveis e outros recursos utilizados na movimentação física do processo;
- Incremento no nível de segurança associado ao Processo Judicial, uma vez que controles de segurança adequados são capazes de oferecer maior grau de dificuldade quanto à adulteração do conteúdo dos processos e quanto ao acesso não autorizado, e torna-se mais simples a criação de cópias de segurança dos processos e seu armazenamento em localidade diferente daquela onde se encontra a versão original.

Uma vez conquistado este avanço do ponto de vista da legislação existente, os diversos órgãos do Poder Judiciário já estão aptos a iniciar a modificação de seus sistemas processuais, e oferecer à sociedade os modernos recursos que viabilizam a instituição do Processo Judicial Eletrônico.

3.4. O fim da era papel no STJ

Muito embora o Processo Judicial Eletrônico já seja regulamentado, por lei, desde dezembro de 2006, sua efetiva adoção não ocorreu de pronto, em função não somente da necessidade do desenvolvimento de soluções de Tecnologia da Informação que o viabilizassem, como também de sua aceitação pela alta direção dos diversos órgãos do Poder Judiciário.

O Superior Tribunal de Justiça, sob a presidência do Exmo. Ministro Francisco Cesar Asfor Rocha, definiu como uma de suas prioridades, para o biênio 2008-2010, a instituição do Processo Judicial Eletrônico. Com efeito, o Plano de Gestão para o referido biênio afirma que *"As ações de modernização serão buscadas com afinco, especialmente no que diz respeito à virtualização dos processos judiciais."*

O mesmo Plano de Gestão, elaborado com base na metodologia BSC (Balanced Scorecard), procura materializar esta intenção em Objetivos Estratégicos e Metas relacionadas, conforme detalhamento abaixo:

- Objetivo Estratégico: Contribuir para a Modernização do Judiciário
    - Meta 15: Virtualizar todos os processos judiciais no STJ, até dezembro de 2010
        - Indicador: Índice de processos virtualizados
        - Situação em dezembro de 2007: Nenhum processo virtualizado
        - Meta para dezembro de 2009: Todos os processos digitalizados
        - Meta para dezembro de 2010: Integral informação do processo judicial
    - Meta 16: Integrar as informações processuais com os 33 tribunais, até dezembro de 2010
        - Indicador: Número de tribunais integrados
        - Situação em dezembro de 2007: 7 Tribunais
        - Meta para dezembro de 2009: 29 Tribunais
        - Meta para dezembro de 2010: 33 Tribunais

Os Objetivos e Metas Estratégicas acima, por sua vez, foram desdobrados em ações concretas. Desta forma, o Processo Judicial Eletrônico foi formalmente instituído no STJ por

meio da Resolução n° 1, de 06/02/2009, que, por sua vez deu origem ao Projeto “Processo Eletrônico”, que se subdividiu em três projetos de tecnologia:

1. i-STJ (integração):

   Visa a integração de dados e informações processuais entre o Superior Tribunal de Justiça, os Tribunais de Justiça, Defensoria Pública, Ministério Público da União, Advocacia-Geral da União e todos os entes públicos que se relacionam com o STJ no intercâmbio de processos e informações processuais.

   Seu principal produto é um sistema de digitalização de processos, já desenvolvido pelo STJ e disponibilizado aos Tribunais que enviam processos diretamente ao próprio STJ, permitindo seu envio já em meio eletrônico, via rede de comunicação de dados.

2. t-STJ (tramitação):

   Visa a instituição do Processo Judicial Eletrônico em sua totalidade, no âmbito do STJ. É projetado para receber os processos oriundos de outros tribunais já em formato digitalizado, a partir do projeto i-STJ, para viabilizar a produção dos atos processuais de competência do STJ já em meio digital, bem como para realizar a tramitação interna do processo exclusivamente em meio eletrônico.

   Além do recebimento de novos processos já em meio digital, sua implantação também possibilitou a digitalização de todos os processos que já haviam sido encaminhados ao STJ, visando o atendimento da Meta 15 anteriormente citada.

3. e-STJ:

   Possibilita o acesso do jurisdicionado, ou seja, advogados, partes, e demais entes públicos participantes do processo, à própria integra do Processo Judicial Eletrônico, viabiliza o Peticionamento Eletrônico, e permite ainda o acesso ao Diário de Justiça Eletrônico (DJ-e), onde são publicadas as decisões finais sobre os processos.

O conjunto dos projetos acima citados, tão logo esteja concluído, efetivamente permitirá o fim da utilização do papel no tocante ao Processo Judicial, no âmbito do STJ.

3.5. Impacto do Processo Judicial Eletrônico na área de Tecnologia da Informação

Conforme citado anteriormente, a implantação do Processo Judicial Eletrônico transforma o papel desempenhado pela Tecnologia da Informação, que passa de um papel secundário a um papel principal, uma vez que os processos passarão a existir apenas em meio digital.

Tal transformação traz diversos impactos na área de TI, com início na área de sistemas, em função da necessidade do desenvolvimento de novas aplicações, passando pela área de atendimento ao usuário, responsável pelas tarefas de treinamento e atendimento propriamente dito, alcançando também a área de infraestrutura, responsável por prover o ambiente de servidores, armazenamento e de comunicação de dados.

Em função do assunto tratado neste trabalho, devemos nos concentrar especialmente no impacto sobre a área de infraestrutura. Para que possamos analisar corretamente a dimensão deste impacto, entretanto, faz-se necessário o conhecimento do universo de Processos Judiciais envolvidos neste novo cenário.

Em nosso auxílio, lançamos mão das estatísticas oficiais do Superior Tribunal de Justiça, que nos mostram a quantidade de processos recebidos e distribuídos anualmente, desde a criação do Tribunal, em 1989, até o ano de 2008.

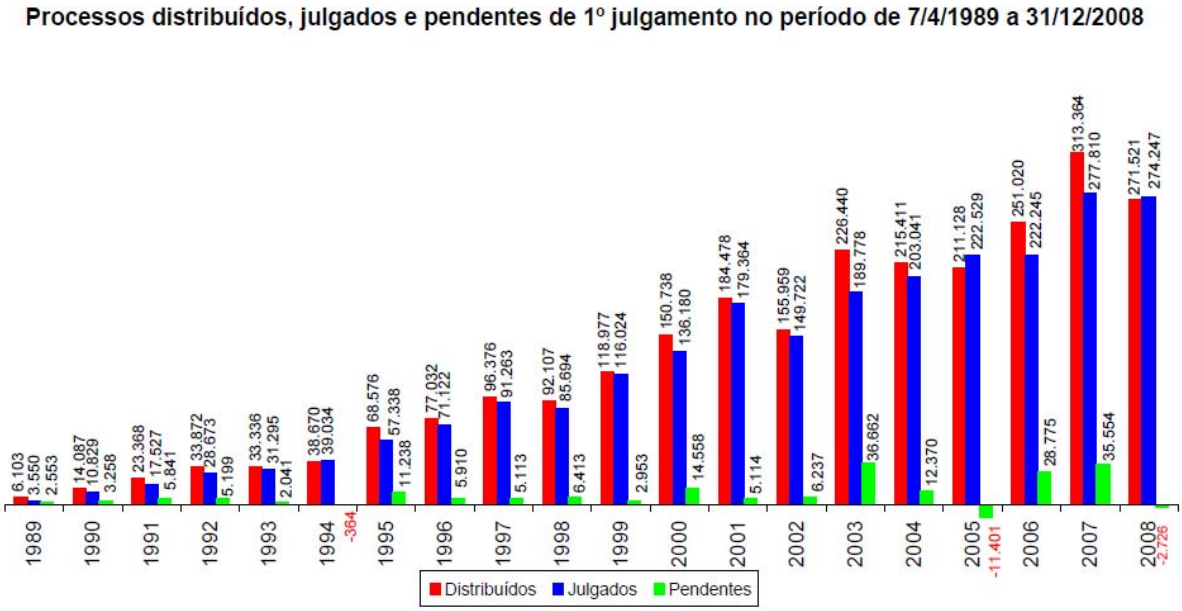

Figura 3.2 – Processos distribuídos, julgados e pendentes de 1º julgamento no período de 7/4/1989 a 31/12/2008. Fonte : Relatório Estatístico – Ano 2008 – Superior Tribunal de Justiça

A figura 2.2 nos mostra que, desde 2003, a quantidade de processos anualmente distribuídos aos Ministros do STJ vem se mantendo acima do patamar de 200.000 unidades. Levando-se em consideração que, em média, cada processo possui 400 páginas, chegamos ao número de 80.000.000 de páginas, por ano, que devem ser armazenadas e potencialmente acessadas, tanto internamente, por unidades do próprio Tribunal, quanto externamente, pelos advogados e partes interessadas nos processos.

Como a grande massa de processos, neste início de implantação, é referente a processos em papel, que devem ser digitalizados para sua utilização como processo eletrônico, o produto da digitalização destes documentos é de especial interesse para o dimensionamento do impacto da mudança de cenário.

A atual tecnologia de digitalização de documentos, que oferece mecanismos de limpeza do produto final, eliminando informações desnecessárias para a representação do documento original com boa qualidade, é capaz de armazenar uma página digitalizada ocupando aproximadamente 250 Kbytes no sistema de armazenamento, o que significa dizer que, por ano, serão necessários cerca de 19 Terabytes para o armazenamento da totalidade dos processos distribuídos.

Tal quantidade de dados traz importantes considerações referentes à infraestrutura necessária, tanto no tocante ao seu armazenamento propriamente dito, ao longo dos anos, como também no que se refere ao sistema de cópias de segurança (back-ups), à capacidade dos equipamentos servidores envolvidos, e à capacidade de comunicação de dados tanto da rede corporativa quanto das redes que interligam o STJ aos demais Tribunais, além das próprias conexões entre o STJ e a Internet.

Com relação à capacidade de armazenamento, devem ser consideradas a quantidade de processos distribuídos por ano bem como os requisitos de temporalidade referentes ao arquivamento dos processos já tramitados em julgado, ou seja, a quantidade de tempo que tais processos devem ser armazenados para fins legais.

As considerações referentes às cópias de segurança (backup) são diretamente dependentes dos requisitos de armazenamento, e devem prever tecnologias capazes de efetuá-las sem causar impacto na disponibilidade exigida para o ambiente do Processo Judicial Eletrônico.

Os equipamentos servidores envolvidos no ambiente devem ser corretamente dimensionados para fazer frente ao aumento de demanda de processamento.

Já a capacidade das redes de comunicação de dados deve se adaptar ao aumento de demanda por tráfego de rede que será experimentado, uma vez que todas as peças processuais serão armazenadas em meio eletrônico, e, consequentemente serão frequentemente consultadas tanto pelas diversas unidades internas do STJ quanto pelos advogados e partes interessadas.

Além das considerações sobre a capacidade necessária para suportar o novo cenário, as questões relacionadas à segurança do ambiente também são de especial importância, concentrando-se nos requisitos de disponibilidade, integridade, confidencialidade, autenticidade e não-repúdio dos atos processuais.

Enquanto os últimos quatro requisitos são mais ligados a soluções adotadas na implementação dos Sistemas de Informação utilizados pelo Processo Judicial Eletrônico, tais como Certificação Digital, Criptografia e procedimentos de verificação e validação das

informações inseridas no processo, o primeiro requisito, disponibilidade, é função de responsabilidade direta do setor de infraestrutura, e é alvo das melhores práticas preconizadas pelo processo DS04 do COBIT, "Assegurar a Continuidade dos Serviços".

Os requisitos de disponibilidade associados ao Processo Judicial Eletrônico podem ser depreendidos do próprio texto da Lei 11.419/2006:

> *Art. 14. Os sistemas a serem desenvolvidos pelos órgãos do Poder Judiciário deverão usar, preferencialmente, programas com código aberto,* ***acessíveis ininterruptamente*** *por meio da rede mundial de computadores, priorizando-se a sua padronização (grifo nosso)*

Outros dois artigos complementam ainda este requisito:

> *Art 3°. …*
> *Parágrafo único. Quando a petição eletrônica for enviada para atender prazo processual, serão consideradas tempestivas as transmitidas até as 24 (vinte e quatro) horas do seu último dia.*

> *Art. 10. …*
> *§ 1º Quando o ato processual tiver que ser praticado em determinado prazo, por meio de petição eletrônica, serão considerados tempestivos os efetivados até as 24 (vinte e quatro) horas do último dia.*

Conforme podemos observar, a lei define o índice de 100% como requisito de disponibilidade. Ainda que este índice de disponibilidade seja virtualmente impossível de ser alcançado, o Superior Tribunal de Justiça vem envidando esforços no sentido de alcançar a maior disponibilidade possível.

Como pano de fundo para a Análise de Maturidade do processo DS04, o próximo ítem deste capítulo discorrerá sobre as medidas de continuidade adotadas no âmbito do Processo Judicial Eletrônico.

3.6. Medidas de Continuidade adotadas no âmbito do Processo Judicial Eletrônico

As medidas de continuidade adotadas podem ser divididas em dois grandes grupos: Arquitetura de Infraestrutura, englobando medidas relacionadas à seleção, aquisição e implantação de arquitetura de equipamentos e software destinada a garantir o nível de disponibilidade requerido, e Organização dos Processos de Trabalho, contemplando medidas relacionadas aos processos de trabalho adotados para garantir que a operação da arquitetura implantada também esteja de acordo com o mesmo nível de disponibilidade.

a) Arquitetura de Infraestrutura

Podemos subdividir a Arquitetura de Infraestrutura em quatro grupos principais: Ambiente Físico, Arquitetura de Servidores, Sistema de Armazenamento e Arquitetura de Redes de Comunicação. A seguir, temos o detalhamento da solução adotada para cada um destes grupos.

- **Ambiente Físico:**

  Até o advento do Processo Judicial Eletrônico, o Superior Tribunal de Justiça contava apenas com um Datacenter, que abrigava todos os seus equipamentos servidores, já dualizados, quer em tecnologia de “clusters” quer em tecnologia de balanceamento de carga, e a totalidade de seu sistema de armazenamento, e não atendia às normas de segurança aplicáveis a este tipo de ambiente. Uma Análise de Riscos realizada sobre o ambiente de Tecnologia da Informação do Tribunal indicou a necessidade tanto da adaptação do Datacenter existente aos padrões de segurança requeridos, quanto da disponibilização de um ambiente de contingência.

  Como primeiro passo foi então construído o ambiente físico de contingência, sob o modelo de Sala-cofre. A existência de dois ambientes físicos proporcionará a implantação do conceito de espelhamento de serviços entre os dois ambientes, oferecendo maior resiliência dos serviços de TI associados ao Processo Judicial Eletrônico no caso da ocorrência de sinistros envolvendo qualquer dos dois ambientes físicos.

Tão logo o ambiente de contingência se torne operacional, o Datacenter original será adaptado de forma a atender aos requisitos de segurança aplicáveis.

- **Arquitetura de Servidores:**

  O STJ vem gradativamente substituindo a tradicional arquitetura de servidores baseada exclusivamente em equipamentos físicos para a arquitetura baseada em virtualização. Desta forma, serviços baseados em equipamentos físicos contarão com um equipamento em cada Datacenter, operando em regime de "cluster", e serviços baseados em servidores virtualizados contarão com um ou mais servidores de virtualização em cada Datacenter, e contarão com os benefícios de continuidade oferecidos por este ambiente, que é capaz de oferecer a movimentação automática de um determinado servidor virtual para outro servidor de virtualização no caso da ocorrência de problemas no servidor original, e contarão também com os benefícios de performance relacionados à distribuição dinâmica de carga de processamento entre os diversos servidores físicos que compõem a solução.

- **Sistema de Armazenamento:**

  O Sistema de Armazenamento, originalmente composto por um único equipamento do tipo "Storage", foi acrescido de mais um equipamento idêntico, que deverá ser sincronizado ao equipamento original por intermédio de ferramentas nativas ao sistema. Os equipamentos do tipo Storage serão instalados um em cada Datacenter.

  Adicionalmente, o sistema de backup, também originalmente composto por um único robô de fitas do tipo LTO, também receberá mais um equipamento, e os backups serão executados de forma cruzada, isto é, o robô de fitas localizado em um Datacenter será responsável pelo backup dos equipamentos localizados no Datacenter remoto, sendo válido também o raciocínio inverso.

  Por fim, levando-se em consideração a natureza dos documentos que compõem o Processo Judicial Eletrônico, que, uma vez produzidos e inseridos no processo, não podem ser alterados ou excluídos, foi adquirida também uma

solução de armazenamento apropriada, identificada pelo mercado como "WORM disk". Tal solução é baseada em discos do tipo WORM (Write Once Read Many, ou Grave uma Vez e Leia Diversas Vezes), que apresentam custo por unidade de armazenamento inferior às soluções tradicionais, e adicionalmente oferecem o benefício de proteção contra alteração ou exclusão dos dados armazenados segundo sua tabela de temporalidade. Assim como as demais soluções de armazenamento adotadas, cada Datacenter terá um equipamento do tipo "WORM disk" instalado.

- **Arquitetura de Redes de Comunicação:**

  Para prover o nível de disponibilidade requerido, a rede de comunicação de dados deve prover interligação entre os Datacenters, de forma a possibilitar a sincronização dos dados armazenados e a realização dos backups cruzados. Adicionalmente a rede local que suporta as estações de trabalho deve estar conectada a ambos os Datacenters.

  A infraestrutura de rede adquirida suporta tais requisitos, interligando os Datacenters sobre um canal de dados de 30 Gbps, e interligando cada prédio da sede do STJ a cada um dos Datacenters a uma velocidade de 10 Gbps.

  Os principais servidores de rede, por sua vez, serão conectados ao switch principal de cada Datacenter através de um link também de 10 Gbps.

  A conexão com a Internet é realizada por intermédio de dois circuitos de comunicação contratados junto a operadoras distintas, de forma a garantir disponibilidade em caso de falha de um dos circuitos, ou mesmo do backbone de uma das operadoras.

  Apenas a conexão com os demais Tribunais é realizada sobre um único circuito de comunicação, parte da Rede de Alta Velocidade da Justiça Federal, contratada e operada pelo Conselho Nacional de Justiça.

b) Organização dos Processos de Trabalho.

A continuidade dos serviços de Tecnologia da Informação não é fruto apenas de uma Arquitetura de Infraestrutura bem definida e implementada, mas também de processos de trabalho que levem em consideração os requisitos de disponibilidade que devem ser alcançados.

No que se refere a este assunto, o Superior Tribunal de Justiça tem uma série de processos de trabalho definidos sob o escopo de um Sistema de Gerenciamento de Segurança da Informação (SGSI), certificado sob a norma ISO/IEC 27001:2005.

Os detalhes da norma ISO/IEC 27001:2005, bem como o caminho trilhado pelas organizações, incluindo neste escopo o STJ, para a obtenção da certificação já foram abordados no capítulo 2. Desta forma, listamos resumidamente os processos organizações orientados conforme recomendações da norma:

- **Análise de Impacto no Negócio:**
  Os diversos ativos de Tecnologia da Informação abrangidos pelo SGSI são classificados em termos de criticidade para o negócio, possibilitando a priorização de ações em termos de segurança.

- **Definição da Gestão de Continuidade de Negócios:**
  São definidos os papéis e responsabilidades associados à Gestão de Continuidade de Negócios com foco em recursos de Tecnologia da Informação, além das Atividades de Contingência e Níveis de Acionamento em decorrência de incidentes.

- **Plano de Recuperação de Desastres:**
  Cada ativo possui um Plano de Recuperação de Desastres associado, detalhando os responsáveis pelo ativo, os procedimentos necessários para recuperação, bem como o tempo de recuperação esperado.

4. METODOLOGIA DA PESQUISA

Este capítulo descreve os procedimentos metodológicos utilizados neste estudo de caso.

A pesquisa é um procedimento sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos e assim contribuir com o conhecimento científico, conectando os dados empíricos às questões iniciais de estudo através de uma seqüência lógica que permitirá chegar às conclusões pretendidas.

4.1. Objetivos da Pesquisa

Os principal objetivo da presente pesquisa é:

- Apresentar um diagnóstico de maturidade das medidas de continuidade aplicadas ao Processo Judicial Eletrônico, no STJ, à luz do processo DS4 e de seus objetivos de controle, propostos pelo COBIT.

4.2. O Problema da Pesquisa

- Quais são os níveis de maturidade para as medidas de continuidade da infraestrutura de TI do Processo Eletrônico do STJ observados sob a ótica do processo DS4 descrito no COBIT?

4.3. Natureza da Pesquisa

Neste trabalho, a pesquisa se caracteriza como sendo de natureza quantitativa, pois busca-se apurar opiniões e atitudes explícitas e conscientes dos entrevistados, utilizando instrumentos estruturados (questionários).

4.4. Estratégia da Pesquisa

A elaboração da estratégia da pesquisa foi precedida de um estudo detalhado da estrutura do COBIT, de forma a determinar que recursos oferecidos pelo modelo seriam úteis para o alcance dos objetivos propostos.

O documento principal do modelo, “Cobit 4.1 – Framework, Control Objectives, Management Guidelines, Maturity Models”, nos apresenta o Apêndice VIII (CobiT e Produtos Relacionados), definindo sua estrutura principal e relacionando trabalhos derivados desta estrutura, dentre os quais destacamos o “IT Assurance Guide: Using CobiT”, que oferece instruções sobre como o COBIT pode ser utilizado para suportar uma série de atividades de Verificação de Conformidade, e oferece sugestões de testes para todos os Processos e Objetivos de Controle do COBIT.

O “IT Assurance Guide” nos dá uma visão geral sobre o modelo COBIT, conforme a figura 4.1, incluindo uma relação dos produtos oferecidos pelo modelo, que são organizados em três níveis, para oferecer suporte a:

- Corpo Diretor e Executivo;
- Gerência de Negócios e de Tecnologia da Informação;
- Profissionais de Governança, Verificação de Conformidade, Controle e Segurança.

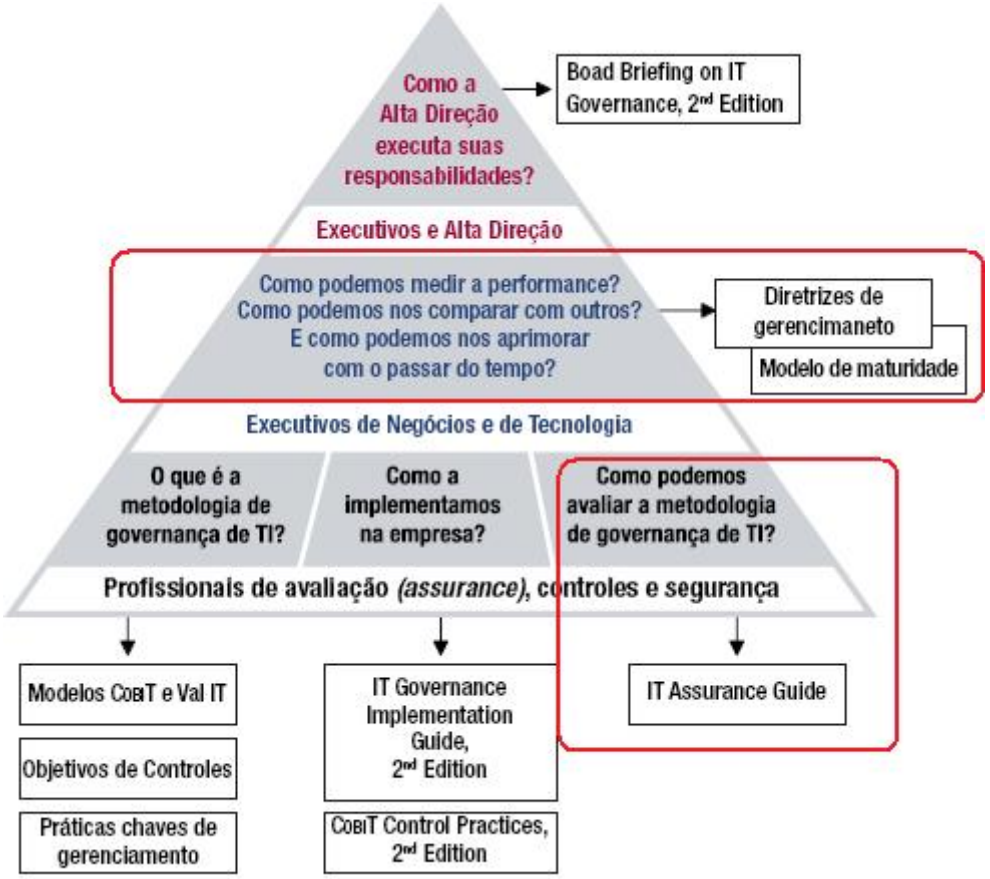

Figura 4.1 – Principais produtos COBIT e sua organização.
Fonte: IT Governance Institute, 2007b, p. 11 - adaptado

As áreas destacadas na Figura 4.1 ressaltam os documentos voltados a medições. Os documentos “Management Guidelines” e “Maturity Models” são aplicáveis para medições de performance, enquanto o “IT Assurance Guide” é aplicável para a avaliação do modelo de governança de TI.

Adicionalmente, o documento “IT Assurance Guide” define ainda uma estratégia genérica para a condução de atividades de verificação de conformidade, tais como o levantamento de nível de maturidade proposto neste trabalho. Esta estratégia genérica é composta por três estágios, descritos abaixo em conjunto com seus passos principais:

I – Planejamento:

a) Estabelecimento de um Universo para a Verificação de Conformidade;

b) Definição do Modelo de Controle a ser utilizado como base para esta verificação.

II – Definição de Escopo:

a) Levantamento dos Objetivos de Negócio e Objetivos de TI;

b) Levantamento dos Processos e Recursos de TI;

c) Definição dos Objetivos de Controle.

III – Execução:

a) Refino da compreensão do objeto da Verificação de Conformidade;

b) Refino do escopo dos Objetivos de Controle chave para o objeto da Verificação de Conformidade;

c) Testar a efetividade do desenho dos principais controles aplicáveis;

d) Alternativamente ou adicionalmente, testar os entregáveis dos principais controles aplicáveis;

e) Documentar o impacto das falhas dos controles;

f) Desenvolver e comunicar as conclusões e recomendações.

Os itens I e II já foram atendidos pela própria proposta deste trabalho, sendo o Universo para Verificação de Conformidade representado pelas Medidas de Continuidade adotadas no âmbito do Processo Eletrônico Judicial, o Modelo de Controle a ser utilizado representado pelo próprio CobiT 4.1, e os itens referentes à Definição do Escopo aqueles constantes do Capítulo 3.

O item III (Execução) é o conjunto de atividades que efetivamente compõem o conteúdo deste Capítulo 4, sendo que os itens “d”, “e” e “f” estão além do escopo definido para este trabalho.

Confrontando as atividades relacionadas nos itens “a”, “b” e “c” com os três documentos destacados na Figura 4.1, chegamos às seguintes conclusões:

a. O Modelo de Maturidade específico para o processo DS4 deve ser utilizado para o mapeamento em alto nível de seu Nível de Maturidade, pois permite, de maneira genérica, o mapeamento da realidade existente sobre o cenário global que define cada um dos níveis de maturidade possíveis;
b. O Nível de Maturidade levantado no passo anterior, entretanto, deve ser confirmado pela análise de conformidade quanto aos Objetivos de Controle

propostos pelo “IT Assurance Guide”, que nos permitirão mapear que controles estão efetivamente sendo praticados pela organização.

Os modelos em questão, entretanto, não oferecem ferramentas prontas para sua aplicação direta em um cenário real. Pesquisamos então por ferramentas e/ou métodos efetivamente utilizados para tal tarefa. Os métodos selecionados estão descritos a seguir:

4.4.1. Mapeamento do Nível de Maturidade do Processo

O método selecionado foi o proposto por Pederiva (2003, p. 2), que parte do princípio da divisão da descrição dos níveis de maturidade em declarações menores, e nos oferece um algoritmo para a determinação do nível de maturidade efetivamente existente na organização.

De acordo com este método, as descrições de cada nível de maturidade do Processo DS4 do COBIT foram subdivididas em declarações, que foram então utilizadas para a elaboração de um questionário referente ao Nível de Maturidade do processo DS4, conforme nos mostram os exemplos na Tabela 4.1, a seguir:

Exemplo da construção do questionário para o processo DS4 (níveis de maturidade 0 e 1)	
Descrição do nível de maturidade	**Declarações**
0 Inexistente - Não há compreensão dos riscos, vulnerabilidades e ameaças às operações de TI ou ao impacto da perda de serviços de TI para o negócio. A continuidade do serviço não é considerada necessária para a administração.	- Existe uma percepção dos riscos, vulnerabilidades e ameaças às operações de TI? - Existe uma percepção do impacto da perda de serviços de TI para o negócio? - A continuidade do serviço é considerada necessária para a administração?
1 Inicial/ *Ad hoc* - As responsabilidades para o serviço contínuo são informais e a autoridade para executar responsabilidades é limitada. A gerência está se tornando ciente dos riscos relacionados ao serviço contínuo e por sua necessidade. O foco da atenção do gerenciamento em serviço contínuo está nos recursos de infraestrutura, ao invés de estar nos serviços de TI. Os usuários implementam contornos em resposta às interrupções de serviços. A resposta da TI às principais interrupções é reativa e despreparada. As interrupções planejadas são programadas para alcançar necessidades da TI, porém, não consideram requisitos do negócio	- As responsabilidades para o serviço contínuo são informais? - Autoridade para executar responsabilidades é limitada? - A gerência está se tornando ciente dos riscos relacionados ao serviço contínuo e por sua necessidade? - O foco da atenção do gerenciamento em serviço contínuo está nos recursos de infraestrutura, ao invés de estar nos serviços de TI? - Os usuários implementam contornos em resposta às interrupções de serviços? - A resposta da TI às principais interrupções é reativa e despreparada? - As interrupções planejadas são programadas para alcançar necessidades da TI, porém, não consideram requisitos do negócio?

Tabela 4.1 – Exemplo da construção do questionário para o processo DS4

O questionário completo referente à Avaliação de Maturidade do Processo DS4 encontra-se no (Apêndice “B”), e contém 42 questões, divididas entre os 6 Níveis de Maturidade possíveis, sendo que cada questão pode ser respondida como “Sim”, “Parcialmente”, “Pouco” ou “Não”.

Para efeito de cálculo do Nível de Maturidade, as respostas são então mapeadas para valores numéricos, conforme peso definidos na Tabela 4.2:

Valores numéricos atribuídos para a conformidade	
Resposta	**Valor**
Não	0
Pouco	0,33
Parcial	0,66
Sim	1

Tabela 4.2 – Valores para determinar a conformidade

Após respondidos os questionários, cada Nível de Maturidade terá, então, valores associados a cada uma de suas questões, como, por exemplo, o Nível de Maturidade 2, exposto na Tabela 4.3:

Nível de maturidade: 2 Repetitivo, mas intuitivo						
Nº da Questão	**Descrição**	**Não**	**Pouco**	**Parcial**	**Sim**	**Valor**
1	A responsabilidade para assegurar continuidade de serviços de TI é formalmente atribuída?			X		0,66
2	As estratégias para assegurar continuidade de serviços de TI tratam isoladamente os serviços e sistemas críticos?				X	1
3	Os relatórios sobre disponibilidade dos sistemas são esporádicos, incompletos e não levam em conta o impacto sobre o negócio?				X	1
4	Existe compromisso da gerência quanto a continuidade de serviços de TI?				X	1
5	Existe um inventário de sistemas e componentes críticos?			X		0,66
					Total	4,32

Tabela 4.3 – Valores de conformidade para o Nível de Maturidade 2

Para cada Nível de Maturidade, o valor “Total” é dividido por sua respectiva quantidade de questões, de forma a se determinar seu valor de conformidade.

Após a realização deste cálculo para cada um dos Níveis de Maturidade, chegamos à Tabela 4.4, que consolida todos os valores de conformidade:

Nível de maturidade	**Soma dos valores de conformidade das questões (A)**	**Total de questões de cada nível de maturidade (B)**	**Valor de Conformidade de cada nível de maturidade (C = A / B)**
0			
1			
2			
3			
4			
5			

Tabela 4.4 – Cálculo dos valores de conformidade da maturidade

Os Valores de Conformidade de cada nível de maturidade (quarta coluna da Tabela 4.4) são então normalizados, de forma a oferecer uma visão da “contribuição” de cada cenário de nível de maturidade ao nível de maturidade geral da organização, conforme a Tabela 4.5:

Nível de maturidade	**Valores de conformidade (C)**	**Valores de conformidade normalizados C / Soma(C)**
0		
1		
2		
3		
4		
5		
Total		

Tabela 4.5 – Cálculo do vetor de conformidade normalizado

Por fim, o Nível de Maturidade referente ao Processo é computado multiplicando-se cada Nível de Maturidade (D) por seu valor de conformidade normalizado (E), somando ao final o valor de todas as contribuições, conforme Tabela 4.6:

Nível de maturidade (D)	**Valores de conformidade normalizados (E)**	**Contribuição (D * E)**
0		
1		
2		
3		
4		
5		
Nível de Maturidade do Processo		

Tabela 4.6 – Cálculo do nível de maturidade do processo

4.4.2. Análise de Maturidade dos Objetivos de Controle

O documento *It Assurance Guide,* em seus Apêndices II, III, IV e V, oferece instruções específicas sobre a avaliação de cada um dos objetivos de controle, nas seções intituladas *"Test the Control Design"* (em tradução livre, Teste o Desenho dos Controles).

Uma pesquisa por métodos de aplicação prática destas instruções nos apresentou o modelo proposto por Rodrigues e Silva (2008), que também parte do princípio da divisão dos cenários descritos no "IT Assurance Guide" em declarações atômicas, com consequente mapeamento dos valores de conformidade de cada Objetivo de Controle, e cálculo final do Nível de Maturidade do Processo.

Desta forma, as recomendações encontradas nas seções *"Test the Control Design"* foram subdivididas em declarações menores, que foram então utilizadas para a elaboração de um questionário para a Avaliação de Maturidade dos Objetivos de Controle do Processo DS4. Tal questionário, cuja íntegra encontra-se no Apêndice "A", contém 52 questões, divididas pelos 10 Objetivos de Controle.

Exemplo da construção do questionário para o objetivo de controle DS4.1 do processo DS4	
Descrição do teste de desenho do controle	**Declarações convertidas em questões**
- Averigue e confirme que organização possui um processo de gestão de continuidade de negócios e que este foi aprovado pelo executivo de TI; - Verifique a análise de impacto de negócios mais atual e determine se o planejamento da continuidade resultou no posicionamento claro dos recursos necessários para recuperar as operações do negócio durante uma interrupção; - Verificar o framework de continuidade de negócios para confirmar que ele inclui todos os elementos necessários para continuar o processo de negócio em caso de uma interrupção (considerar a responsabilidade, comunicação, plano de escalonamento, estratégias de recuperação, os níveis de serviço de TI e de negócios, e os procedimentos de emergência).	- Um processo para gerenciamento da continuidade de serviços de TI foi definido? - O processo para gerenciamento da continuidade de serviços de TI foi aprovado pela Secretaria de Tecnologia? - O plano de continuidade de TI definiu claramente os componentes necessários para recuperar os serviços relacionados ao processo eletrônico durante um incidente? - O framework de continuidade inclui todos os elementos necessários para restabelecer os serviços de TI, incluindo dentre eles os relacionados ao processo eletrônico, no caso de interrupção (considerando responsabilidades, plano de comunicação, plano de escalação, estratégias de recuperação, níveis de serviço da TI e do negócio, e procedimentos emergenciais)?

Tabela 4.7 – Exemplo da construção do questionário para o objetivo de controle DS4.1 do processo DS4

As respostas consolidadas dos questionários foram confrontadas ao Modelo de Maturidade Genérico proposto pelo CobiT, descrito no item 2.5 deste trabalho. Os resultados obtidos para cada Objetivo de Controle foram comparados aos Níveis de Maturidade, em uma escala decrescente, do nível 5 para o nível 0. O Nível de Maturidade que fosse completamente atendido por um Objetivo de Controle deve ser o nível a ele atribuído.

O Nível de Maturidade do Processo, então, é calculado como uma média dos Níveis de Maturidade atribuídos a cada Objetivo de Controle.

4.4.3. Seleção do público-alvo para resposta aos questionários

Conforme indicado no item 2.4 deste trabalho, o processo DS4 possui papéis e responsabilidades definidos sem ambigüidades, de acordo com o modelo RACI.

Os papéis e responsabilidades apresentados na figura 2.8, de maneira genérica, para todas as organizações, foram mapeadas para os cargos e funções existentes no STJ, de acordo com a relação abaixo:

- **CIO** – Secretário de Tecnologia da Informação e das Comunicações
- **HEAD OPERATIONS** – Seção de Operação e Serviços
- **BUSINESS PROCESS OWNER** – demais Seções da Coordenadoria de Infraestrutura e Produção (Banco de Dados, Gerência de Rede, Segurança de Rede, Serviços Corporativos e Sistemas Operacionais)
- **CHIEF ARCHITECT** – Responsável pelo Sistema de Gestão de Segurança da Informação (SGSI)
- **HEAD DEVELOPMENT** – Coordendador de Desenvolvimento
- **HEAD IT ADMINISTRATION** – Coordenador de Infraestrutura e Produção
- **PMO** – Central de Apoio a Projetos

As demais funções citadas no gráfico RACI da figura 2.8 não foram consideradas, uma vez que as iniciativas referentes à Continuidade de Serviços no STJ ainda são restritas à Secretaria de Tecnologia da Informação.

Os questionários foram elaborados com o auxílio da ferramenta “Formulários” do Google Docs, e então encaminhados aos ocupantes dos cargos e funções acima relacionados, a seus substitutos, ao grupo responsável pelo SGSI, composto por 3 pessoas, e a todos os componentes da Seção de Operação e Serviços, pois esta é a unidade diretamente envolvida na execução de todas as tarefas de produção referentes aos diversos sistemas da organização, incluindo aquelas relativas ao Processo Judicial Eletrônico. O Centro de Apoio a Projetos não foi incluído dentre os escolhidos para participação na pesquisa uma vez que o SGSI vem sendo implementado sem sua participação.

No total, os questionários foram enviados a 22 pessoas, tendo sido recebidos 19 questionários preenchidos. Os dados automaticamente consolidados pela ferramenta do Google Docs foram mapeados em tabelas de frequência, exibidas nos Apêndices “D” e “E”. Os valores mais frequentes foram utilizados para popular os quadros finais utilizados na Análise de Dados, objeto do próximo item deste trabalho.

5. ANÁLISE DE DADOS

O presente capítulo descreve os resultados da análise dos dados pesquisados, levantados a partir da aplicação dos dois questionários (Apêndices A e B). O objetivo primordial é propiciar o entendimento do nível de maturidade do processo DS4. Aqui são detalhados os resultados da pesquisa, possibilitando a avaliação do nível de maturidade de cada um dos dez objetivos de controle do processo DS4, bem como a maturidade do processo propriamente dito.

5.1. Análise do nível de maturidade do processo DS4

Uma vez respondidos todos os questionários, suas repostas foram tabuladas de maneira a determinar as opções mais frequantemente assinaladas, de acordo com o Apêndice "D". As opções mais frequentes foram então utilizadas para o preenchimento dos quadros relativos aos diversos níveis de maturidade possíveis, quadros estes apresentados no Apêndice "E".

Cada Nível de Maturidade teve então seu valor de conformidade calculado conforme descrito no item 4.4.1 deste trabalho, e estes valores de conformidade foram então transportados para a segunda coluna da Tabela 5.1.

Nível de maturidade	Soma dos valores de conformidade das questões (A)	Total de questões de cada nível de maturidade (B)	Valor de Conformidade de cada nível de maturidade (C=A/B)
0	0,00	3,00	0,00
1	4,97	8,00	0,62
2	4,32	5,00	0,86
3	4,98	8,00	0,62
4	1,66	8,00	0,21
5	1,32	9,00	0,15

Tabela 5.1 – Cálculo dos valores de conformidade da maturidade

De acordo com o modelo proposto por Pederiva (2003), estes valores devem então ser normalizados, para posterior cálculo da contribuição de cada nível de maturidade ao valor final calculado, conforme demonstram as Tabelas 5.2 e 5.3.

Nível de maturidade	Valores de conformidade não normalizados (C)	Valores de conformidade normalizados [C/Soma(C)]
0	0,00	0,00
1	0,62	0,25
2	0,86	0,35
3	0,62	0,25
4	0,21	0,09
5	0,15	0,06
Total	**2,46**	**1,00**

Tabela 5.2 – Cálculo do vetor de conformidade normalizado

Nível de maturidade (D)	Valores de conformidade normalizados (E)	Contribuição (D * E)
0	0,00	0,00
1	0,25	0,25
2	0,35	0,70
3	0,25	0,75
4	0,09	0,36
5	0,06	0,30
Nível de Maturidade do Processo DS4		**2,36**

Tabela 5.3 – Cálculo da maturidade do Processo DS4 no STJ

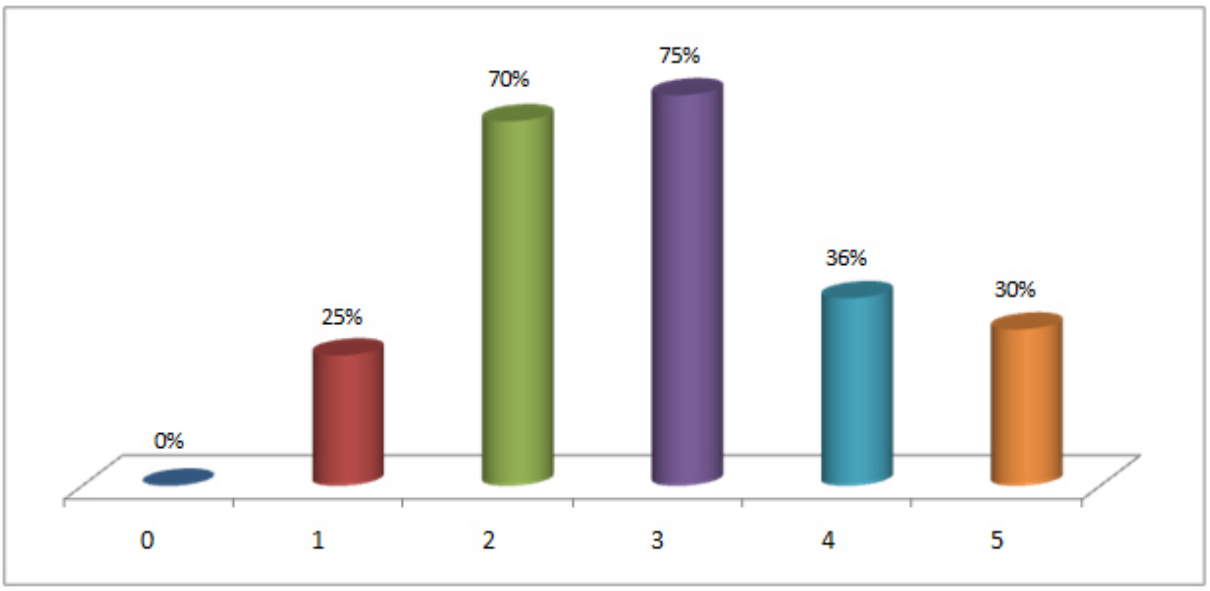

Figura 5.1 – Nível de Maturidade do Processo DS4 do COBIT no STJ

O resultado final observado, bem como a identificação dos fatores que contribuiram mais fortemente para este resultado, evidenciam que as medidas de Continuidade de Serviço referentes ao Processo Judicial Eletrônico efetivamente apresentam maturidade oscilando entre os níveis 2 e 3. Como apenas a parte inteira do resultado final deve ser considerada para a definição do nível de maturidade, devemos afirmar que o Processo DS4 no âmbito do Processo Judicial Eletrônico do STJ encontra-se no Nível de Maturidade 2, já apresentando, entretanto, características dos níveis 3, 4 e em estado ainda inicial, também do nível 5.

Em uma tradução livre, a descrição do nível 2 é a seguinte: *"A responsabilidade pela garantia de continuidade dos serviços é atribuída. As abordagens para garantia de continuidade dos serviços são fragmentadas. Relatórios sobre a disponibilidade dos sistemas são esporádicos, podem ser incompletos e não levam em consideração impactos sobre o negócio. Não há nenhum Plano de Continuidade documentado, embora haja comprometimento com a continuidade dos serviços e seus princípios mais importantes sejam conhecidos. Existe um inventário sobre os sistemas e componentes críticos, embora possa não ser confiável. Práticas relativas a continuidade estão surgindo, mas o sucesso depende de indivíduos."*

As principais deficiências que ainda impedem que o processo atinja o Nível de Maturidade 3 são falhas nas definições de responsabilidade sobre planejamento e testes de continuidade, a inexistência de relatórios periódicos sobre os testes de continuidade, falhas na

comunicação da necessidade de planejamento por parte da gerência e, por fim, a falta de confiabilidade do inventário de sistemas e componentes críticos.

Como pontos positivos, porém, já pertencentes aos níveis de maturidade 3 e 4, podemos destacar a existência de um plano de continuidade de TI documentado, ainda que pouco divulgado, porém alinhado à criticidade dos sistemas para o negócio, a atribuição da responsabilidade de manter o planto de continuidade de TI, e o correto funcionamento dos componentes de alta disponibilidade e redundância.

5.2. Análise do nível de maturidade dos objetivos de controle DS4.1 a DS4.10

5.2.1. Análise do objetivo de controle DS4.1 - Framework de Continuidade de TI

O objetivo de controle DS4.1 recomenda o desenvolvimento de um framework para a continuidade de TI suportar a gestão de continuidade de negócios de toda a organização, utilizando um processo consistente. O objetivo do framework deve ser ajudar a determinar o nível de resiliência necessária da infraestrutura tecnológica e impulsionar o desenvolvimento de planos de recuperação de desastre e planos de contingência de TI. O framework deverá abordar a estrutura organizacional para a gestão da continuidade, abrangendo as funções, tarefas e responsabilidades dos provedores de serviços internos e externos, sua gestão e os seus clientes, bem como os processos de planejamento que criam as regras e estruturas para documentar, testar e executar a recuperação de desastres os planos de contingência de TI. O plano deverá ainda abordar itens como a identificação de recursos críticos, anotando dependências chave, a monitoração e a comunicação da disponibilidade de recursos críticos, alternativa de processamento, e os princípios de backup e recuperação.

As respostas às questões relativas a este objetivo de controle, apresentadas no questionário (APÊNDICE A), apresentaram a seguinte distribuição de acordo com frequência absoluta máxima das opções disponíveis (APÊNDICE F):

Questões	**Respostas com maior frequência**
1 - Um processo para gerenciamento da continuidade de serviços de TI foi definido?	**SIM**
2 - O processo para gerenciamento da continuidade de serviços de TI foi aprovado pela Secretaria de Tecnologia?	**SIM**
3 - O plano de continuidade de TI definiu claramente os componentes necessários para recuperar os serviços relacionados ao processo eletrônico durante um incidente?	**SIM**
4 - O framework de continuidade inclui todos os elementos necessários para restabelecer os serviços de TI, incluindo dentre eles os relacionados ao processo eletrônico, no caso de interrupção (considerando responsabilidades, plano de comunicação, plano de escalação, estratégias de recuperação, níveis de serviço da TI e do negócio, e procedimentos emergenciais)?	**NÃO**

Conforme explicado no Capítulo 4, a definição do nível de maturidade a partir da avaliação dos objetivos de controle é realizada comparando-se as respostas obtidas com a definição do modelo genérico de maturidade do CobiT. Busca-se uma aproximação a partir das respostas obtidas e das evidências observadas com a definição do nível de maturidade, iniciando no nível 5 e descendo até o nível 0 do modelo.

A análise mostra que o objetivo de controle DS4.1 situa-se no estágio de maturidade 2 (repetitivo mas intuitivo). A principal constatação que levou a atribuição deste nível foi o observação que o Plano de Continuidade de TI do STJ existe, mas que não há divulgação adequada para todos os envolvidos.

5.2.2. Análise do objetivo de controle DS4.2 - Planos de Continuidade de TI

O objetivo de controle DS4.2 recomenda que sejam desenvolvidos planos de continuidade de TI baseados no framework, concebidos para reduzir o impacto de uma interrupção significativa nas funções chave do negócio. Os planos devem ser baseados na compreensão dos riscos dos potenciais impactos nos negócios e endereçar os requisitos de resiliência, alternativa de processamento e capacidade de recuperação de todos os serviços críticos de TI. Devem também abranger diretrizes de uso, os papéis e responsabilidades, procedimentos, processos de comunicação, e a abordagem de teste.

As respostas às questões relativas a este objetivo de controle, apresentadas no questionário (APÊNDICE A), apresentaram a seguinte distribuição de acordo com frequência absoluta máxima das opções disponíveis (APÊNDICE F):

Questões	**Respostas com maior frequência**
1 - Existem planos de continuidade para os sistemas e serviços mais importantes?	**SIM**
2 - Cada plano de continuidade define formas de processamento alternativo?	**SIM**
3 - Cada plano de continuidade define capacidade de recuperação alinhada ao impacto do serviço?	**NÃO**
4 - Cada plano define regras e responsabilidades?	**SIM**
5 - Cada plano inclui processos de comunicação?	**SIM**
6 - Cada plano define uma configuração de recuperação mínima aceitável?	**SIM**
7 - Existe uma estratégia de testes para os planos de continuidade?	**NÃO**
8 - Os testes dos planos de continuidade estão sendo executados em uma freqüência combinada entre as áreas?	**NÃO**
9 - Os resultados dos testes são analisados?	**NÃO**

Segundo os dados obtidos na pesquisa, o objetivo de controle DS4.2 situa-se no estágio de maturidade 3 (gerenciado). Este nível foi atribuído considerando que existem planos de continuidade de TI para os serviços mais importantes, onde são definidos procedimentos, responsabilidades e processos de comunicação, mas que ainda não estão alinhados aos impactos no negócio e não possuem abordagem de teste.

5.2.3. Análise do objetivo de controle DS4.3 - Recursos Críticos de TI

O objetivo de controle DS4.3 recomenda centrar a atenção nos itens especificados como mais críticos no plano de continuidade de TI, para a construção de resiliência e estabelecimento de prioridades em situações de recuperação. Deve-se evitar a distração de recuperação de ativos menos críticos e garantir uma resposta e recuperação em conformidade com as necessidades prioritárias do negócio, assegurando que os custos são mantidos em um nível aceitável e que cumpram os requisitos regulatórios e contratuais. Deve-ser considerar diferentes níveis de resiliência, resposta e necessidades de recuperação, por exemplo, de uma a quatro horas, de quatro a 24 horas, mais de 24 horas e os períodos operacionais críticos para os negócios.

As respostas às questões relativas a este objetivo de controle, apresentadas no questionário (APÊNDICE A), apresentaram a seguinte distribuição de acordo com frequência absoluta máxima das opções disponíveis (APÊNDICE F):

Questões	**Respostas com maior frequência**
1 - Existe um inventário dos serviços e sistemas e seus respectivos níveis de criticidade?	**NÃO**
2 - Os sistemas e serviços mais críticos possuem planos de continuidade, suportando processos e recursos?	**SIM**
3 - Os planos de continuidade foram definidos de acordo com os objetivos do negocio e conformidade legal?	**SIM**
4 - Os planos de continuidade foram testados de acordo com os objetivos do negocio e conformidade legal?	**NÃO**
5 - Existe um processo para assegurar a consistência entre os vários planos de continuidade dos sistemas e serviços críticos?	**NÃO**

A análise mostra que o objetivo de controle DS4.3 situa-se no estágio de maturidade 1 (inicial/ad hoc). A principal constatação que levou a atribuição deste nível foi que apesar da existência de planos de continuidade de TI para os serviços mais críticos, a falta do inventário atrapalha a consistência do processo, sendo agravado pela ausência dos procedimentos de testes, fato que torna o resultado do processo incerto.

5.2.4. Análise do objetivo de controle DS4.4 - Manutenção do Plano de Continuidade de TI

O objetivo de controle DS4.4 recomenda incentivar a gestão de TI para definir e executar procedimentos de controle de mudanças que garantirão que o plano de continuidade seja mantido atualizado e refletindo continuamente os requisitos atuais do negócio. Deve-se comunicar as alterações nos procedimentos e responsabilidades de forma clara e em tempo hábil.

As respostas às questões relativas a este objetivo de controle, apresentadas no questionário (APÊNDICE A), apresentaram a seguinte distribuição de acordo com frequência absoluta máxima das opções disponíveis (APÊNDICE F):

Questões	**Respostas com maior frequência**
1 - Todas as cópias do plano de continuidade de TI são revisadas e atualizadas periodicamente?	**SIM**
2 - Todas as cópias são armazenadas on-site e off-site?	**SIM**
3 - Todas as mudanças criticas dos recursos de TI são comunicadas para o gerente de continuidade para atualização do plano de continuidade?	**NÃO**
4 - As mudanças no plano de continuidade são realizadas em intervalos regulares?	**NÃO**
5 - As mudanças no plano de continuidade seguem procedimentos de controle de alteração?	**SIM**

Segundo os dados obtidos na pesquisa, o objetivo de controle DS4.4 situa-se no estágio de maturidade 2 (repetitivo mas intuitivo), visto que os procedimentos para atualização do plano de continuidade de TI foram definidos, apesar da periodicidade não ser a ideal diante da dinâmica das mudanças ocorridas na infraestrutura. O processo de comunicação da ocorrência de mudanças que deveriam ser refletidas nos planos não está sendo realizado.

5.2.5. Análise do objetivo de controle DS4.5 - Teste do Plano de Continuidade de TI

O objetivo de controle DS4.5 recomenda testar o plano de continuidade de TI regularmente para assegurar que os sistemas de TI possam ser efetivamente recuperados, as deficiências deverão ser corrigidas para garantir que o plano permanece relevante. Esse controle requer uma preparação cuidadosa, consulta à documentação e comunicação dos resultados do teste e, de acordo com os resultados, a implementação de um plano de ação. Deve-se considerar cenários de testes para a recuperação de aplicações simples bem como cenários de teste de recuperação de aplicações integradas, fim-a-fim.

As respostas às questões relativas a este objetivo de controle, apresentadas no questionário (APÊNDICE A), apresentaram a seguinte distribuição de acordo com frequência absoluta máxima das opções disponíveis (APÊNDICE F):

Questões	**Respostas com maior frequência**
1 - Os testes de continuidade de TI são agendados e aplicados regularmente após alterações da infraestrutura de TI e das aplicações?	**NÃO**
2 - Novos componentes e atualizações são incluídos no agendamento de testes do plano de continuidade?	**NÃO**
3 - Um agendamento de teste foi criado e inclui detalhes do teste para garantir uma seqüência lógica e real das interrupções?	**NÃO**
4 - Uma equipe para realizar testes foi definida?	**NÃO**
5 - As pessoas envolvidas nos testes são diferentes daquelas responsáveis pela execução do plano de continuidade?	**NÃO**
6 - É verificada junto à equipe a definição de uma alternativa quando os testes não são viáveis?	**NÃO**
7 - O sucesso ou falha do teste é medido e reportado e a mudança é realizada no plano de continuidade?	**NÃO**
8 - Os resultados são revisados para determinar a eficácia da operação?	**NÃO**

A análise mostra que o objetivo de controle DS4.5 situa-se no estágio de maturidade 0 (inexistente). A principal constatação que levou a atribuição deste nível foi que embora o Superior Tribunal de Justiça disponha de um Plano de Continuidade documentado, não há evidências da existência de rotinas de testes deste plano, o que pode ocasionar diversos

problemas como desconhecimento de deficiências existentes nos planos de recuperação, dados desatualizados que não refletem o ambiente atual e etapas inadequadas de recuperação dos processos de TI. Todos estes problemas podem resultar em incapacidade de recuperação em caso de verdadeiro desastre.

5.2.6. Análise do objetivo de controle DS4.6 - Treinamento do Plano de Continuidade de TI

O objetivo de controle DS4.6 recomenda proporcionar a todos os interessados treinamento regular dos procedimentos, papéis e responsabilidades em caso de incidentes ou desastre. Deve-se verificar a necessidade de aumento da freqüência dos treinamentos de acordo com os resultados dos testes do plano de contingência.

As respostas às questões relativas a este objetivo de controle, apresentadas no questionário (APÊNDICE A), apresentaram a seguinte distribuição de acordo com frequência absoluta máxima das opções disponíveis (APÊNDICE F):

Questões	**Respostas com maior frequência**
1 - São realizados treinamentos referentes aos procedimentos de continuidade de serviços regularmente?	**NÃO**
2 - A necessidade de treinamento e o agendamento são avaliados e atualizados regularmente?	**NÃO**
3 - A lista, agendamento e material de treinamento são revisados para determinar a eficácia da operação?	**NÃO**
4 - Programas para divulgar projetos de continuidade de TI estão sendo realizados em todos os níveis?	**NÃO**

Segundo os dados obtidos na pesquisa, o objetivo de controle DS4.6 situa-se no estágio de maturidade 1 (inicial / ad hoc), visto que novos colaboradores recebidos na área de infraestrutura recebem treinamento referente ao Sistema de Gerenciamento de Segurança da Informação, entretanto não existe um programa de treinamento regular relativo aos procedimentos e os papéis e responsabilidades dos envolvidos no caso de um incidente ou desastre.

5.2.7. Análise do objetivo de controle DS4.7 - Distribuição do Plano de Continuidade de TI

O objetivo de controle DS4.7 recomenda implementar e gerenciar uma estratégia de distribuição para garantir que os planos de continuidade sejam adequadamente distribuídos, de forma segura, para os interessados devidamente autorizados, quando e onde for necessário. Deve ser dada atenção para tornar os planos acessíveis em todos os cenários de desastres.

As respostas às questões relativas a este objetivo de controle, apresentadas no questionário (APÊNDICE A), apresentaram a seguinte distribuição de acordo com frequência absoluta máxima das opções disponíveis (APÊNDICE F):

Questões	**Respostas com maior frequência**
1 - Uma lista de distribuição para o plano de continuidade de TI foi definida?	**SIM**
2 - O procedimento de distribuição foi avaliado?	**NÃO**
3 - Todas as cópias digitais e físicas do plano estão protegidas?	**SIM**
4 - Os documentos são acessados somente por pessoas autorizadas?	**SIM**

A análise mostra que o objetivo de controle DS4.7 situa-se no estágio de maturidade 3 (gerenciado), visto que o Plano de Continuidade de TI está documentado, armazenado eletronicamente em um CMS (Content Management System) que dispõe de controle de acesso, e também é distribuído aos responsáveis em cópias impressas. Entretanto não há garantias de que todas as cópias estejam efetivamente protegidas, podendo ocorrer o vazamento de informações por pessoas não autorizadas.

5.2.8. Análise do objetivo de controle DS4.8 - Recuperação e Retomada de Serviços de TI

O objetivo de controle DS4.8 recomenda planejar as ações a serem tomadas no momento em que a equipe de TI necessitará realizar a retomada e recuperação dos serviços. Isso pode incluir a ativação de sites de backup, a iniciação da alternativa de processamento, a comunicação com os clientes e as partes interessadas, e procedimentos de retomada. Garantir que a organização compreende o momento de recuperação da TI e as necessidades de investimentos em tecnologia necessária para apoiar as necessidades de recuperação dos negócios.

As respostas às questões relativas a este objetivo de controle, apresentadas no questionário (APÊNDICE A), apresentaram a seguinte distribuição de acordo com frequência absoluta máxima das opções disponíveis (APÊNDICE F):

Questões	**Respostas com maior frequência**
1 - Para os casos de incidente, os procedimentos incluem todos os passos para a avaliação dos danos, bem como trata dos pontos formais de decisões necessários para a ativação dos planos de continuidade?	**SIM**
2 - Os planos de recuperação correspondem aos requisitos do negócio?	**SIM/ NÃO SEI**

Segundo os dados obtidos na pesquisa, nesta questão houve empate entre o nº de resposta Sim e Não sei, evidenciando falha na divulgação dos procedimentos de recuperação e retomada. Considerando este cenário identificou-se que o objetivo de controle DS4.8 situa-se no estágio de maturidade 2 (repetitivo mas intuitivo), visto que o plano de recuperação contém os procedimentos necessários para recuperar os sistemas críticos, porém a falta de conhecimento por parte de todos os envolvidos poderá inviabilizar que isso ocorra no tempo demandado pela área de negócio.

5.2.9. Análise do objetivo de controle DS4.9 - Armazenamento do backup em outros locais

O objetivo de controle DS4.9 recomenda armazenar fora das instalações principais todas as mídias críticas de backup, itens de documentação e outros recursos necessários para a recuperação de TI, bem como os planos de continuidade de negócios. Determinar o teor de armazenamento de backup em colaboração c com os proprietários dos processos de negócios e de TI. A equipe de gestão da unidade de armazenamento externo deve conhecer e aplicar a política de classificação de dados e as práticas corporativas de gerenciamento de mídias de armazenamento. O gerenciamento de TI deve assegurar que o armazenamento externo é avaliado periodicamente, pelo menos uma vez ao ano, quanto à segurança, questões ambientais e gestão do conteúdo. Deve-se garantir a compatibilidade de hardware e software para restaurar os dados arquivados, e periodicamente testar e atualizar os dados arquivados.

As respostas às questões relativas a este objetivo de controle, apresentadas no questionário (APÊNDICE A), apresentaram a seguinte distribuição de acordo com frequência absoluta máxima das opções disponíveis (APÊNDICE F):

Questões	**Respostas com maior frequência**
1 - Os dados estão protegidos quando estão em um sistema de armazenamento off site?	**SIM**
2 - Os dados estão protegidos quando transportados?	**NÃO**
3 - Os dados estão protegidos quando estão no local de armazenamento alternativo?	**SIM**
4 - Os procedimentos de teste foram revisados para determinar a eficácia da operação?	**NÃO SEI**
5 - A mídia de backup contém toda a informação necessária para o plano de continuidade de TI?	**NÃO SEI**
6 - Existem instruções de recuperação suficientes?	**SIM**
7 - Existe um inventário dos backups e mídias?	**SIM**
8 - É verificado se esse inventário está correto?	**NÃO SEI**

A análise mostra que o objetivo de controle DS4.9 situa-se no estágio de maturidade 2 (repetitivo mas intuitivo), visto que os dados de backup necessários para a recuperação dos

sistemas estão protegidos em local distante do CPD, porém não existe a certeza de que num cenário de desastre seja possível recuperar os sistemas a partir destes backups, o que pode acarretar em perda irremediável de dados.

5.2.10. Análise do objetivo de controle DS4.10 - Revisão Pós-retomada

O objetivo de controle DS4.10 recomenda determinar que a equipe de gestão de TI estabeleça procedimentos para a avaliação da adequação do plano em relação à retomada eficaz da função de TI após um desastre, atualizando o plano nesse sentido.

As respostas às questões relativas a este objetivo de controle, apresentadas no questionário (APÊNDICE A), apresentaram a seguinte distribuição de acordo com frequência absoluta máxima das opções disponíveis (APÊNDICE F):

Questões	**Respostas com maior frequência**
1 - As falhas do plano se tornam focos importantes para a adequação e atualização do plano de continuidade?	**Não**
2 - Após efetuar recuperações, são realizadas reuniões para discutir melhorias?	**Não**
3 - Planos, políticas e procedimentos foram revisados para determinar a eficácia da operação?	**Não**

Segundo os dados obtidos na pesquisa, o objetivo de controle DS4.10 situa-se no estágio de maturidade 0 (inexistente), visto que a falta do processo de testes e conseqüentemente a não revisão do plano de continuidade provoca a descrença na sua efetividade por parte do envolvidos no processo de retomada. Essa situação tem como resultado a avaliação que os planos de recuperação não estão adequados, não atendendo seus objetivos e deixando de atender as necessidades do negócio.

5.2.11. Cálculo do valor da maturidade do processo DS4 a partir das maturidades dos objetivos de controle

A figura 5.2 representa a distribuição dos níveis de maturidade obtidos para cada objetivo de controle do processo DS4.

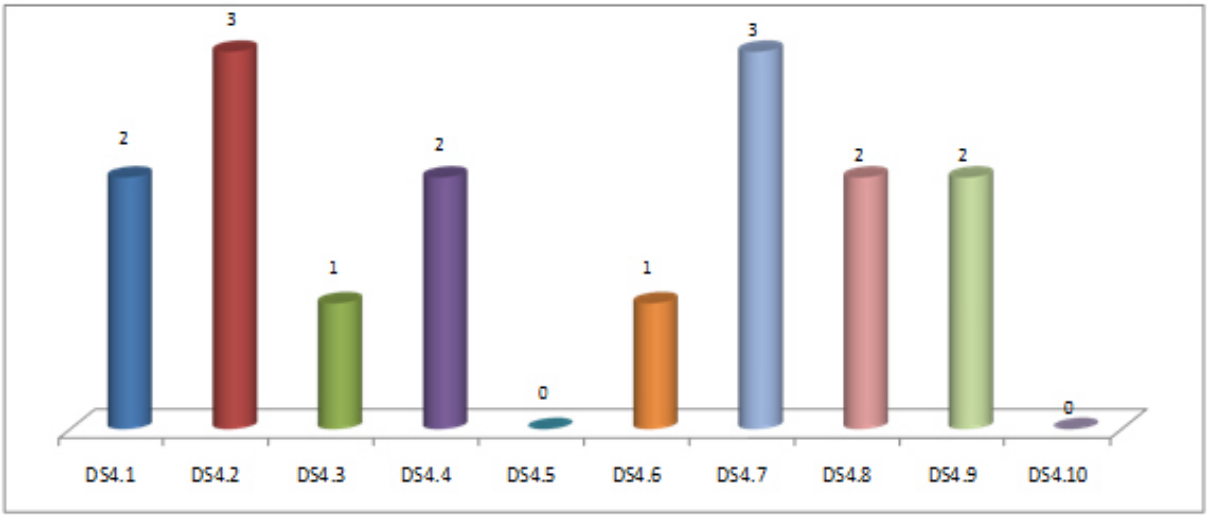

Figura 5.2 – Nível de Maturidade dos Objetivos de Controle do Processo DS4 do COBIT no STJ

Conforme explicado no Capítulo 4, a definição do nível de maturidade a partir da avaliação dos objetivos de controle é obtida a partir da media aritmética dos Níveis de Maturidade atribuídos a cada Objetivo de Controle, conforme apresentado na tabela 5.4.

Objetivos de Controle do Processo DS4	Nível de Maturidade do Objetivo de Controle obtido a partir da avaliação do desenho do controle
DS4.1	2
DS4.2	3
DS4.3	1
DS4.4	2
DS4.5	0
DS4.6	1
DS4.7	3
DS4.8	2
DS4.9	2
DS4.10	0
Nível de Maturidade do Processo DS4	**1,6**

Tabela 5.4 – Cálculo da maturidade do processo a partir da avaliação do desenho do controle

6. CONCLUSÃO

A Análise de Maturidade do Processo DS4 apresentou como resultado um Nível de Maturidade superior ao resultado obtido pela Análise de Maturidade dos Objetivos de Controle. Tal fato se explica em função do caráter mais subjetivo do primeiro método, em que se mede a percepção dos entrevistados com relação à maturidade do processo, em oposição ao caráter mais objetivo do segundo, que verifica se os controles necessários estão sendo efetivamente aplicados ao processo, configurando-se um método mais rígido.

Entretanto, pudemos observar que ambas as análises confirmam mutuamente seus resultados. Os objetivos de controle que obtiveram pior avaliação foram o DS4.3 (Recursos Críticos de TI), DS4.5 (Teste do Plano de Continuidade de TI) e DS4.10 (Revisão Pós-retomada), resultado consistente com as principais deficiências levantadas pela avaliação de maturidade do processo, destacadas no item 5.1 deste trabalho.

A partir da avaliação obtida, o próprio modelo COBIT provê, no documento *"CobiT Control Practices – Guidance do Achieve Control Objectives for Successful IT Governance"*, práticas de controle que devem ser implementadas para que possam ser atingidos cada um dos níveis de maturidade definidos, viabilizando, portanto, a elaboração de um Plano de Melhorias que permita à organização alcançar o nível de maturidade desejado, em função de suas expectativas e de seus recursos disponíveis.

Com relação aos métodos aplicados, podemos afirmar que a Análise de Maturidade do Processo, conforme proposto por Pederiva (2003), provê um resultado de mais alto nível, que deve ser complementado pela análise dos Objetivos de Controle para que se obtenha uma melhor noção dos controles que efetivamente estejam em operação. Esta análise dos Objetivos de Controle pode, por sua vez, ser complementada pelas seguintes atividades:

- Coleta de evidências que comprovem as respostas fornecidas;
- Teste dos resultados efetivos dos objetivos de controle; e
- Documentação dos impactos causados pelas deficiências dos controles.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. *NBR ISO/IEC 27001:2006 – Sistema de Gestão de Segurança da Informação - Requisitos.* Rio de Janeiro, 2006.

BALANCED SCORECARD INSTITUTE. Disponível em http://www.balancedscorecard.org. Acesso em: 17/10/2009.

BASTOS, Alberto; CAUBIT, Rosângela. *ISO 27001 e 27002: gestão de segurança da informação – uma visão prática*. Editora Zoulk, 2009.

CARVALHO FILHO, Sergio de. *Estatística básica: teoria e 150 questões*. Editora Elsevier, 2005.

CONSELHO NACIONAL DE JUSTIÇA, Metas Nacionais de Nivelamento, ano de 2009. Disponível em: http://www.cnj.jus.br/images/stories/docs_cnj/resolucao/rescnj_70_ii.pdf. Acesso em 17/11/2009.

Constituição da República Federativa do Brasil de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/constitui%C3%A7ao.htm. Acesso em: 15/11/2009.

DE LA TORRE, Wagner Giron. *A morosidade da Justiça e a defunção dos direitos. Jus Navigandi*, Teresina, ano 6, n. 58, ago. 2002. Disponível em: http://jus2.uol.com.br/doutrina/texto.asp?id=3038. Acesso em: 15/11/2009.

FERNANDES, Aguinaldo A.; ABREU, Vladimir F. *Implantando a Governança de TI da Estratégia à Gestão dos Processos e Serviços*. Rio de Janeiro: BRASPORT, 2006.

FREITAS, Cecília de Souza. *Considerações acerca do Processo Judicial Eletrônico. R2 Learning.* Disponível em: http://www.r2learning.com.br/_site/artigos/curso_oab_concurso_artigo_784_Consideracoes_acerca_do_Processo_Judicial_Eletronico. Acesso em: 15/11/2009.

IT GOVERNANCE INSTITUTE. *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit.* Illinois: IT Governance Institute, 2008.

IT GOVERNANCE INSTITUTE. *Board Briefing on IT Governance, 2nd Edition.* Illinois: IT Governance Institute, 2003.

IT GOVERNANCE INSTITUTE. *CobiT framework*. Ilinois: IT Governance Institute, 2007a.

IT GOVERNANCE INSTITUTE. *CobiT Mapping: Overview Of International It Guidance, 2nd Edition.* Illinois: IT Governance Institute, 2006.

IT GOVERNANCE INSTITUTE. Disponível em http://www.itgovernance.org. Acesso em: 15/10/2009.

IT GOVERNANCE INSTITUTE. *IT Assurance Guide using CobiT*. Illinois: IT Governance Institute, 2007b.

Lei N° 11.419, de 19 de dezembro de 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 15/11/2009.

Metodologia para Avaliação de Maturidade de Processos COBIT 4.1. Disponível em http://www.confidentia.srv.br/Downloads/Metodologia.pdf. Acesso em 15/11/209

PEDERIVA, Andrea. *The COBIT Maturity Model in a Vendor Evaluation Case*. Information Systems Control Journal, Volume 3, 2003. Disponível em: http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=15925. Acesso em: 04/11/2009.

PIOVESAN, Flavia. *Direitos Humanos e o Direito Constitucional Internacional*. Editora Max Limonad, 1996.

Plano de Gestão do Superior Tribunal de Justiça – Biênio 2008-2010. Disponível em: http://www.stj.gov.br/portal_stj/publicacao/download.wsp?tmp.arquivo=1038. Acesso em: 20/11/2009.

Processo Eletrônico. Uma revolução no Judiciário. Disponível em http://ww2.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=368&tmp.texto=92609. Acesso em 15/11/2009.

RAMOS, Anderson (org.). *Security Officer – 1: guia oficial para formação de gestores em segurança da informação*. Editora Zoulk, 2009.

RODRIGUES, Paulo; SILVA, Marcelo. Metodologia para Avaliação de Maturidade de Processos CobiT 4.1 – v9.0. Disponível em http://www.confidentia.srv.br/Downloads/Metodologia.pdf. Acesso em: 02/11/2009.

SOFTWARE ENGINEERING INSTITUTE. Disponível em http://www.sei.cmu.edu/cmmi/index.cfm. Acesso em: 17/10/2009.

WEILL, Peter; ROSS, Jeanne W. *Governança de TI: como as empresas com melhor desempenho administram os direitos decisórios de TI na busca por resultados superiores.* M. Books do Brasil, 2006.

APÊNDICES

APÊNDICE A – QUESTIONÁRIO I: AVALIAÇÃO DE MATURIDADE DOS OBJETIVOS DE CONTROLE DO PROCESSO DS4.

Avaliação de maturidade dos objetivos de controle do processo DS4 do COBIT

Prezado colega,

O processo DS4 do CobiT possui 10 Objetivos de Controle associados. O presente questionário visa determinar em que medida cada um deles se encontra implementado no STJ. Recomendamos a leitura atenta de cada pergunta para que o resultado final seja o mais fiel possível à realidade.

Agradecemos novamente por sua colaboração!

* Obrigatório

Preenchido por: *

Área: *

Cargo: *

DS4.1 Framework de Continuidade de TI

Desenvolver um framework para continuidade de TI para apoiar o gerenciamento global de continuidade do negócio de toda a empresa utilizando um processo consistente. O objetivo do framework é ajudar em determinar o poder de recuperação requerido da infraestrutura e direcionar o desenvolvimento de recuperação de desastre e planos de contingência de TI. O framework deve direcionar a estrutura organizacional para gerenciamento de continuidade, cobrindo os papéis, tarefas e responsabilidades de fornecedores de serviço internos e externos, sua gerência e seus clientes, e as regras e estruturas para documentar, testar e executar planos de recuperação de desastre e de contingência de TI. O plano também deve abordar itens como a identificação de recursos críticos, monitoração e relatório de disponibilidade de recursos críticos, processamento alternativo, e os princípios de backup e recuperação

1 - Um processo para gerenciamento da continuidade de serviços de TI foi definido? *

Sim

Não

Não sei

2 - O processo para gerenciamento da continuidade de serviços de TI foi aprovado pela Secretaria de Tecnologia? *

Sim

Não

Não sei

3 - O plano de continuidade de TI definiu claramente os componentes necessários para recuperar os serviços relacionados ao processo eletrônico durante um incidente? *

Sim

Não

Não sei

4 - O framework de continuidade inclui todos os elementos necessários para restabelecer os serviços de TI, incluindo dentre eles os relacionados ao processo eletrônico, no caso de interrupção (considerando responsabilidades, plano de comunicação, plano de escalação, estratégias de recuperação, níveis de serviço da TI e do negócio, e procedimentos emergenciais)? *

Sim

Não

Não sei

DS4.2 Planos de Continuidade de TI

Desenvolver planos de continuidade de TI com base no framework e desenhados para reduzir o impacto de uma interrupção severa nas funções e processos chave do negócio. Os planos devem ser baseados no entendimento dos riscos dos potenciais impactos no negócio e tratar os requisitos sobre poder de recuperação, processamento alternativo e capacidade de recuperação de todos os serviços críticos de TI. Eles também devem cobrir diretrizes de uso, papéis e responsabilidades, procedimentos, processos de comunicação, e a abordagem de teste.

1 - Existem planos de continuidade para os sistemas e serviços mais importantes? *

Sim

Não

Não sei

2 - Cada plano de continuidade define formas de processamento alternativo? *

Sim

Não

Não sei

3 - Cada plano de continuidade define capacidade de recuperação alinhada ao impacto do serviço? *

Sim

Não

Não sei

4 - Cada plano define regras e responsabilidades? *

Sim

Não

Não sei

5 - Cada plano inclui processos de comunicação? *

Sim

Não

Não sei

6 - Cada plano define uma configuração de recuperação mínima aceitável? *

Sim

Não

Não sei

7 - Existe uma estratégia de testes para os planos de continuidade? *

Sim

Não

Não sei

8 - Os testes dos planos de continuidade estão sendo executados em uma freqüência combinada entre as áreas? *

Sim

Não

Não sei

9 - Os resultados dos testes são analisados? *

Sim

Não

Não sei

DS4.3 Recursos Críticos de TI

Focar a atenção em itens especificados como os mais críticos no plano de continuidade de TI para a construção de poder de recuperação e estabelecer prioridades em situações de recuperação. Evitar a atenção na recuperação de itens menos críticos e assegurar resposta e recuperação em alinhamento com necessidades da prioridade do negócio, enquanto é assegurado que custos sejam mantidos em um nível aceitável e concordando com requisitos regulatórios e contratuais. Considerar poder de recuperação, resposta e requisitos de recuperação para faixas diferentes, ex: uma a quatro horas, quatro a 24 horas, mais de 24 horas e períodos operacionais críticos do negócio.

1 - Existe um inventário dos serviços e sistemas e seus respectivos níveis de criticidade? *

Sim

Não

Não sei

2 - Os sistemas e serviços mais críticos possuem planos de continuidade, suportando processos e recursos? *

Sim

Não

Não sei

3 - Os planos de continuidade foram definidos de acordo com os objetivos do negocio e conformidade legal? *

Sim

Não

Não sei

4 - Os planos de continuidade foram testados de acordo com os objetivos do negocio e conformidade legal?

Sim

Não

Não sei

5 - Existe um processo para assegurar a consistência entre os vários planos de continuidade dos sistemas e serviços críticos? *

Sim

Não

Não sei

DS4.4 Manutenção do Plano de Continuidade de TI

Incentivar o gerenciamento de TI a definir e executar procedimentos de controle das mudanças assegurando que o plano de continuidade de TI seja mantido atualizado e reflita continuamente requisitos reais do negócio. É essencial que as mudanças nos procedimentos e nas responsabilidades sejam claramente comunicadas e com uma freqüência oportuna.

1 - Todas as cópias do plano de continuidade de TI são revisadas e atualizadas periodicamente? *

Sim

Não

Não sei

2 - Todas as cópias são armazenadas on-site e off-site? *

Sim

Não

Não sei

3 - Todas as mudanças criticas dos recursos de TI são comunicadas para o gerente de continuidade para atualização do plano de continuidade? *

Sim

Não

Não sei

4 - As mudanças no plano de continuidade são realizadas em intervalos regulares? *

Sim

Não

Não sei

5 - As mudanças no plano de continuidade seguem procedimentos de controle de alteração? *

Sim

Não

Não sei

DS4.5 Teste do Plano de Continuidade de TI

Testar o plano de continuidade de TI em uma base regular para assegurar que sistemas de TI possam ser recuperados eficazmente, suas falhas sejam tratadas e o plano permaneça aplicável. Isto requer preparação cuidadosa, documentação, relatar resultados de teste e, de acordo com os resultados, implementar um plano de ação.

1 - Os testes de continuidade de TI são agendados e aplicados regularmente após alterações da infraestrutura de TI e das aplicações? *

Sim

Não

Não sei

2 - Novos componentes e atualizações são incluídos no agendamento de testes do plano de continuidade? *

Sim

Não

Não sei

3 - Um agendamento de teste foi criado e inclui detalhes do teste para garantir uma seqüência lógica e real das interrupções? *

Sim

Não

Não sei

4 - Uma equipe para realizar testes foi definida? *

Sim

Não

Não sei

5 - As pessoas envolvidas nos testes são diferentes daquelas responsáveis pela execução do plano de continuidade? *

Sim

Não

Não sei

6 - É verificada junto à equipe a definição de uma alternativa quando os testes não são viáveis? *

Sim

Não

Não sei

7 - O sucesso ou falha do teste é medido e reportado e a mudança é realizada no plano de continuidade? *

Sim

Não

Não sei

8 - Os resultados são revisados para determinar a eficácia da operação? *

Sim

Não

Não sei

DS4.6 Treinamento do Plano de Continuidade de TI

Assegurar que todas as partes interessadas recebem sessões de treinamento regular relativo aos procedimentos e seus papéis e responsabilidades no caso de um incidente ou desastre. Verificar e aumentar o treinamento de acordo com os resultados dos testes de contingência.

1 - São realizados treinamentos referentes aos procedimentos de continuidade de serviços regularmente? *

Sim

Não

Não sei

2 - A necessidade de treinamento e o agendamento são avaliados e atualizados regularmente? *

Sim

Não

Não sei

3 - A lista, agendamento e material de treinamento são revisados para determinar a eficácia da operação? *

Sim

Não

Não sei

4 - Programas para divulgar projetos de continuidade de TI estão sendo realizados em todos os níveis? *

Sim

Não

Não sei

DS4.7 Distribuição do Plano de Continuidade de TI

Determinar que exista uma estratégia definida e administrada de distribuição para assegurar que os planos sejam distribuídos corretamente e com segurança e disponíveis às partes interessadas apropriadamente autorizadas quando e onde necessário. Deve-se tomar o cuidado de que os planos estejam acessíveis em todos os cenários de desastre.

1 - Uma lista de distribuição para o plano de continuidade de TI foi definida? *

Sim

Não

Não sei

2 - O procedimento de distribuição foi avaliado? *

Sim

Não

Não sei

3 - Todas as cópias digitais e físicas do plano estão protegidas? *

Sim

Não

Não sei

4 - Os documentos são acessados somente por pessoas autorizadas? *

Sim

Não

Não sei

DS4.8 Recuperação e Retomada de Serviços de TI

Planejar as ações a serem tomadas para o período quando a TI estiver recuperando e retomando serviços. Isto pode incluir a ativação de locais de backup, iniciação de processamento alternativo, comunicação ao cliente e aos stakeholders e procedimentos de retomada. Assegurar que o negócio entenda os tempos de recuperação de TI e os investimentos em tecnologia necessários para suportar as necessidades do negócio quanto à recuperação e retomada.

1 - Para os casos de incidente, os procedimentos incluem todos os passos para a avaliação dos danos, bem como trata dos pontos formais de decisões necessários para a ativação dos planos de continuidade? *

Sim

Não

Não sei

2 - Os planos de recuperação correspondem aos requisitos do negócio? *

Sim

Não

Não sei

DS4.9 Armazenamento de Backup em Outros Locais

Armazenar em locais fora do site todas as mídias críticas de backup, documentação e outros recursos de TI necessários para recuperação da TI e os planos de continuidade do negócio. O conteúdo do armazenamento do backup precisa ser determinado em colaboração entre proprietários do processo do negócio e pessoal de TI. O gerenciamento da facilidade de armazenamento fora do site deve responder à política de classificação de dados e as práticas de armazenamento de mídia da empresa. O gerenciamento de TI deve assegurar que a acomodação em outro local seja periodicamente avaliada, pelo menos anualmente, quanto ao conteúdo, proteção ambiental e a segurança. Assegurar compatibilidade de hardware e software para arquivar dados restaurados e periodicamente testar e renovar dados arquivados.

1 - Os dados estão protegidos quando estão em um sistema de armazenamento offsite? *

Sim

Não

Não sei

2 - Os dados estão protegidos quando transportados? *

Sim

Não

Não sei

3 - Os dados estão protegidos quando estão no local de armazenamento alternativo? *

Sim

Não

Não sei

4 - Os procedimentos de teste foram revisados para determinar a eficácia da operação? *

Sim

Não

Não sei

5 - A mídia de backup contém toda a informação necessária para o plano de continuidade de TI? *

Sim

Não

Não sei

6 - Existem instruções de recuperação suficientes? *

Sim

Não

Não sei

7 - Existe um inventário dos backups e mídias? *

Sim

Não

Não sei

8 - É verificado se esse inventário está correto? *

Sim

Não

Não sei

DS4.10 Revisão Pós-retomada

Na retomada bem sucedida da função de TI depois de um desastre, determinar se o gerenciamento de TI estabeleceu procedimentos para avaliar a adequação do plano e atualização.

1 - As falhas do plano se tornam focos importantes para a adequação e atualização do plano de continuidade? *

Sim

Não

Não sei

2 - Após efetuar recuperações, são realizadas reuniões para discutir melhorias? *

Sim

Não

Não sei

3 - Planos, políticas e procedimentos foram revisados para determinar a eficácia da operação? *

Sim

Não

Não sei

APÊNDICE B - QUESTIONÁRIO II: AVALIAÇÃO DE MATURIDADE DO PROCESSO DS4.

Avaliação de maturidade do processo DS4 do COBIT

Prezado colega,

O questionário abaixo pretende avaliar a sua percepção sobre o nível de maturidade do STJ com relação ao processo DS4 do CobiT (Garantir a continuidade dos serviços). Existem 6 níveis de maturidade possíveis, e as questões estão agrupadas em cada um desses 6 níveis. Desta forma, é possível a existência de perguntas semelhantes dentro de níveis de maturidade distintos. Caso você tenha a impressão de estar respondendo à mesma pergunta novamente, por favor, compare as perguntas e verifique as nuances de cada uma.

Obrigado pela colaboração!

* Obrigatório

DS4 Garantir continuidade dos serviços

A necessidade para a oferta de serviços contínuos de TI requer desenvolvimento, manutenção e planejamento de teste de continuidade de TI, armazenamento de backup fora do local e treinamento periódico do plano de continuidade. Um processo eficaz de serviço contínuo minimiza a probabilidade e impacto de uma interrupção de um serviço importante de TI em funções e processos chave do negócio.

Preenchido por: *

Área: *

Cargo: *

Nível de maturidade: 0 Inexistente

1 - Existe uma percepção dos riscos, vulnerabilidades e ameaças às operações de TI? *

Não

Pouco

Parcialmente

Sim

2 - Existe uma percepção do impacto da perda de serviços de TI para o negócio? *

Não

Pouco

Parcialmente

Sim

3 - A continuidade do serviço é considerada necessária pela a administração? *

Não

Pouco

Parcialmente

Sim

Nível de maturidade: 1 Inicial / Ad hoc

1 - As responsabilidades referentes a continuidade de serviços de TI são informais? *

Não

Pouco

Parcialmente

Sim

2 - A autoridade para execução dos procedimentos de continuidade de serviços de TI é limitada? *

Não

Pouco

Parcialmente

Sim

3 - A gerência tem ciência dos riscos relacionados à continuidade de serviços de TI? *

Não

Pouco

Parcialmente

Sim

4 - A gerência tem ciência da necessidade da continuidade de serviços de TI? *

Não

Pouco

Parcialmente

Sim

5 - O foco da atenção do gerenciamento em continuidade de serviços de TI está nos recursos de infraestrutura, ao invés de estar nos serviços de TI? *

Não

Pouco

Parcialmente

Sim

6 - Os usuários implementam procedimentos de contorno em resposta às interrupções de serviços? *

Não

Pouco

Parcialmente

Sim

7 - A resposta da TI às principais interrupções é reativa e despreparada? *

Não

Pouco

Parcialmente

Sim

8 - As interrupções planejadas são programadas para alcançar necessidades da TI, porém, não consideram requisitos do negócio? *

Não

Pouco

Parcialmente

Sim

Nível de maturidade: 2 Repetitivo, mas intuitivo

1 - A responsabilidade para assegurar continuidade de serviços de TI é formalmente atribuída? *

Não

Pouco

Parcialmente

Sim

2 - As estratégias para assegurar continuidade de serviços de TI tratam isoladamente os serviços e sistemas críticos? *

Não

Pouco

Parcialmente

Sim

3 - Os relatórios sobre disponibilidade dos sistemas são esporádicos, incompletos e não levam em conta o impacto sobre o negócio? *

Não

Pouco

Parcialmente

Sim

4 - Existe compromisso da gerência quanto à continuidade de serviços de TI? *

Não

Pouco

Parcialmente

Sim

5 - Existe um inventário de sistemas e componentes críticos? *

Não

Pouco

Parcialmente

Sim

Nível de matirudade: 3 Processo Definido

1 - As responsabilidades para planejamento e teste de continuidade de serviços de TI estão claramente definidas e atribuídas? *

Não

Pouco

Parcialmente

Sim

2 - O plano de continuidade de TI está documentado? *

Não

Pouco

Parcialmente

Sim

3 - O plano de continuidade de TI é baseado na criticidade do sistema e no impacto do negócio? *

Não

Pouco

Parcialmente

Sim

4 - Há um relatório periódico de teste de continuidade de serviços de TI? *

Não

Pouco

Parcialmente

Sim

5 - Os indivíduos tomam a iniciativa para o seguimento de padrões e recebimento de treinamento para lidar com incidentes importantes ou um desastre? *

Não

Pouco

Parcialmente

Sim

6 - A gerência comunica consistentemente a necessidade de planejamento para assegurar serviço contínuo? *

Não

Pouco

Parcialmente

Sim

7 - Os componentes da alta disponibilidade e da redundância dos sistemas e serviços estão operando corretamente? *

Não

Pouco

Parcialmente

Sim

8 - Um inventário de sistemas e componentes críticos é mantido? *

Não

Pouco

Parcialmente

Sim

Nível de maturidade: 4 Gerenciado e Medido

1 - As responsabilidades e padrões para continuidade de serviços são exigidas da forma como foram definidos? *

Não

Pouco

Parcialmente

Sim

2 - É atribuída a responsabilidade de manter o plano de continuidade de serviços de TI? *

Não

Pouco

Parcialmente

Sim

3 - As atividades de manutenção são baseadas nos resultados de testes de continuidade de serviços de TI, nas boas práticas internas e nas mudanças do ambiente de TI e de negócio? *

Não

Pouco

Parcialmente

Sim

4 - Os dados estruturados sobre continuidade de serviços de TI estão sendo reunidos, analisados, reportados e trabalhados? *

Não

Pouco

Parcialmente

Sim

5 - É oferecido treinamento formal, de forma obrigatória, sobre os processos de continuidade de serviços de TI? *

Não

Pouco

Parcialmente

Sim

6 - As boas práticas da disponibilidade de sistemas e serviços estão sendo aplicadas consistentemente? *

Não

Pouco

Parcialmente

Sim

7 - Os incidentes de descontinuidade são classificados. *

Não

Pouco

Parcialmente

Sim

8 - O caminho crescente de escalonamento para cada um dos incidentes de descontinuidade é bem conhecido por todos os envolvidos? *

Não

Pouco

Parcialmente

Sim

Nível de maturidade: 5 Otimizado

1 - Os processos integrados de continuidade de serviços de TI levam em conta as melhores práticas externas? *

Não

Pouco

Parcialmente

Sim

2 - O plano de continuidade de TI é integrado com os planos de continuidade do negócio? *

Não

Pouco

Parcialmente

Sim

3 - O plano de continuidade de TI é mantido rotineiramente? *

Não

Pouco

Parcialmente

Sim

4 - Os requisitos para assegurar continuidade de serviços de TI são apoiados pelos principais fornecedores? *

Não

Pouco

Parcialmente

Sim

5 - Ocorre teste global do plano de continuidade de TI? *

Não

Pouco

Parcialmente

Sim

6 - Os resultados do teste global são entradas para a atualização do plano de continuidade de serviços de TI? *

Não

Pouco

Parcialmente

Sim

7 - Coleta e análise de dados são usadas para a melhoria contínua do processo? *

Não

Pouco

Parcialmente

Sim

8 - Práticas de disponibilidade e planejamento de continuidade de serviços de TI são alinhados completamente? *

Não

Pouco

Parcialmente

Sim

9 - A gerência assegura que um desastre ou um incidente importante não ocorra como conseqüência de um ponto único de falha? *

Não

Pouco

Parcialmente

Sim

APÊNDICE C – TABELA COM ATRIBUIÇÃO DOS VALORES DE CONFORMIDADE PARA CADA QUESTÃO.

Nível de maturidade: 0 Inexistente					
NÚMERO DA QUESTÃO	**QUESTÃO**	**VALOR DE CONFORMIDADE DA QUESTÃO**			
		NÃO	**POUCO**	**PARCIAL**	**SIM**
1	Existe uma percepção dos riscos, vulnerabilidades e ameaças às operações de TI?	1	0.66	0.33	0
2	Existe uma percepção do impacto da perda de serviços de TI para o negócio?	1	0.66	0.33	0
3	A continuidade do serviço é considerada necessária pela a administração?	1	0.66	0.33	0
Nível de maturidade: 1 Inicial / Ad hoc					
1	As responsabilidades referentes a continuidade de serviços de TI são informais?	0	0.33	0.66	1
2	A autoridade para execução dos procedimentos de continuidade de serviços de TI é limitada?	0	0.33	0.66	1
3	A gerência tem ciência dos riscos relacionados à continuidade de serviços de TI?	0	0.33	0.66	1
4	A gerência tem ciência da necessidade da continuidade de serviços de TI?	0	0.33	0.66	1
5	O foco da atenção do gerenciamento em continuidade de serviços de TI está nos recursos de infraestrutura, ao invés de estar nos serviços de TI?	0	0.33	0.66	1
6	Os usuários implementam procedimentos de contorno em resposta às interrupções de serviços?	0	0.33	0.66	1
7	A resposta da TI às principais interrupções é reativa e despreparada?	0	0.33	0.66	1
8	As interrupções planejadas são programadas para alcançar necessidades da TI, porém, não consideram requisitos do negócio?	0	0.33	0.66	1
Nível de maturidade: 2 Repetitivo, mas intuitivo					
1	A responsabilidade para assegurar continuidade de serviços de TI é formalmente atribuída?	0	0.33	0.66	1
2	As estratégias para assegurar continuidade de serviços de TI tratam isoladamente os serviços e sistemas críticos?	0	0.33	0.66	1
3	Os relatórios sobre disponibilidade dos sistemas são esporádicos, incompletos e não levam em conta o impacto sobre o negócio?	0	0.33	0.66	1
4	Existe compromisso da gerência quanto a continuidade de serviços de TI?	0	0.33	0.66	1
5	Existe um inventário de sistemas e componentes críticos?	0	0.33	0.66	1
Nível de maturidade: 3 Processo Definido					
1	As responsabilidades para planejamento e teste de continuidade de serviços de TI estão claramente definidas e atribuídas?	0	0.33	0.66	1
2	O plano de continuidade de TI está documentado?	0	0.33	0.66	1
3	O plano de continuidade de TI é baseado na criticidade do sistema e no impacto do negócio?	0	0.33	0.66	1

4	Há um relatório periódico de teste de continuidade de serviços de TI?	0	0.33	0.66	1
5	Os indivíduos tomam a iniciativa para o seguimento de padrões e recebimento de treinamento para lidar com incidentes importantes ou um desastre?	0	0.33	0.66	1
6	A gerência comunica consistentemente a necessidade de planejamento para assegurar serviço contínuo?	0	0.33	0.66	1
7	Os componentes da alta disponibilidade e da redundância dos sistemas e serviços estão operando corretamente?	0	0.33	0.66	1
8	Um inventário de sistemas e componentes críticos é mantido?	0	0.33	0.66	1
Nível de maturidade: 4 Gerenciado e Medido					
1	As responsabilidades e padrões para continuidade de serviços são exigidas da forma como foram definidos?	0	0.33	0.66	1
2	É atribuída a responsabilidade de manter o plano de continuidade de serviços de TI?	0	0.33	0.66	1
3	As atividades de manutenção são baseadas nos resultados de testes de continuidade de serviços de TI, nas boas práticas internas e nas mudanças do ambiente de TI e de negócio?	0	0.33	0.66	1
4	Os dados estruturados sobre continuidade de serviços de TI estão sendo reunidos, analisados, reportados e trabalhados?	0	0.33	0.66	1
5	É oferecido treinamento formal, de forma obrigatória, sobre os processos de continuidade de serviços de TI?	0	0.33	0.66	1
6	As boas práticas da disponibilidade de sistemas e serviços estão sendo aplicadas consistentemente?	0	0.33	0.66	1
7	Os incidentes de descontinuidade são classificados?	0	0.33	0.66	1
8	O caminho crescente de escalonamento para cada um dos incidentes de descontinuidade é bem conhecido por todos os envolvidos?	0	0.33	0.66	1
Nível de maturidade: 5 Otimizado					
1	Os processos integrados de continuidade de serviços de TI levam em conta as melhores práticas externas?	0	0.33	0.66	1
2	O plano de continuidade de TI é integrado com os planos de continuidade do negócio?	0	0.33	0.66	1
3	O plano de continuidade de TI é mantido rotineiramente?	0	0.33	0.66	1
4	Os requisitos para assegurar continuidade de serviços de TI são apoiados pelos principais fornecedores?	0	0.33	0.66	1
5	Ocorre teste global do plano de continuidade de TI?	0	0.33	0.66	1
6	Os resultados do teste global são entradas para a atualização do plano de continuidade de serviços de TI?	0	0.33	0.66	1
7	Coleta e análise de dados são usadas para a melhoria contínua do processo?	0	0.33	0.66	1
8	Práticas de disponibilidade e planejamento de continuidade de serviços de TI são alinhados completamente?	0	0.33	0.66	1
9	A gerência assegura que um desastre ou um incidente importante não ocorra como conseqüência de um ponto único de falha?	0	0.33	0.66	1

Tabela C.1 – Tabela com atribuição dos valores de conformidade para cada questão.

APÊNDICE D – ANÁLISE DA FREQUÊNCIA DAS QUESTÕES RELACIONADAS AO PROCESSO DS4

D.1 – Distribuição das frequencias das respostas relacionadas ao nível de maturidade 0 (Inexistente)

1 - Existe uma percepção dos riscos, vulnerabilidades e ameaças às operações de TI?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*0*	*0,0*	*0,0*
Pouco	*1*	*5,3*	*5,3*
Parcialmente	*5*	*26,3*	*31,6*
Sim	*13*	*68,4*	*100,0*
Total	***19***	***100,0***	

Tabela D.1 – Distribuição da frequência das respostas da questão 1 da maturidade 0

2 - Existe uma percepção do impacto da perda de serviços de TI para o negócio?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*0*	*0,0*	*0,0*
Pouco	*0*	*0,0*	*0,0*
Parcialmente	*7*	*36,8*	*36,8*
Sim	*12*	*63,2*	*100,0*
Total	***19***	***100,0***	

Tabela D.2 – Distribuição da frequência das respostas da questão 2 da maturidade 0

3 - A continuidade do serviço é considerada necessária pela a administração?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*0*	*0,0*	*0,0*
Pouco	*1*	*5,3*	*5,3*
Parcialmente	*0*	*0,0*	*5,3*
Sim	*18*	*94,7*	*100,0*
Total	***19***	***100,0***	

Tabela D.3 – Distribuição da frequência das respostas da questão 3 da maturidade 0

D.2 – Distribuição das frequencias das respostas relacionadas ao nível de maturidade 1 (Inicial / Ad hoc)

1 - As responsabilidades referentes à continuidade de serviços de TI são informais?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*5*	*26,3*	*26,3*
Pouco	*4*	*21,1*	*47,4*
Parcialmente	*9*	*47,4*	*94,7*
Sim	*1*	*5,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.4 – Distribuição da frequência das respostas da questão 1 da maturidade 1

2 - A autoridade para execução dos procedimentos de continuidade de serviços de TI é limitada?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*2*	*10,5*	*10,5*
Pouco	*5*	*26,3*	*36,8*
Parcialmente	*7*	*36,8*	*73,7*
Sim	*5*	*26,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.5 – Distribuição da frequência das respostas da questão 2 da maturidade 1

3 - A gerência tem ciência dos riscos relacionados à continuidade de serviços de TI?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*1*	*5,3*	*5,3*
Pouco	*3*	*15,8*	*21,1*
Parcialmente	*6*	*31,6*	*52,6*
Sim	*9*	*47,4*	*100,0*
Total	***19***	***100,0***	

Tabela D.6 – Distribuição da frequência das respostas da questão 3 da maturidade 1

4 - A gerência tem ciência da necessidade da continuidade de serviços de TI?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*0*	*0,0*	*0,0*
Pouco	*1*	*5,3*	*5,3*
Parcialmente	*5*	*26,3*	*31,6*
Sim	*13*	*68,4*	*100,0*
Total	***19***	***100,0***	

Tabela D.7 – Distribuição da frequência das respostas da questão 4 da maturidade 1

5 - O foco da atenção do gerenciamento em continuidade de serviços de TI está nos recursos de infraestrutura, ao invés de estar nos serviços de TI?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*3*	*15,8*	*15,8*
Pouco	*0*	*0,0*	*15,8*
Parcialmente	*9*	*47,4*	*63,2*
Sim	*7*	*36,8*	*100,0*
Total	***19***	***100,0***	

Tabela D.8 – Distribuição da frequência das respostas da questão 5 da maturidade 1

6 - Os usuários implementam procedimentos de contorno em resposta às interrupções de serviços?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*6*	*31,6*	*31,6*
Pouco	*7*	*36,8*	*68,4*
Parcialmente	*2*	*10,5*	*78,9*
Sim	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela D.9 – Distribuição da frequência das respostas da questão 6 da maturidade 1

7 - A resposta da TI às principais interrupções é reativa e despreparada?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*2*	*11,1*	*11,1*
Pouco	*1*	*5,6*	*16,7*
Parcialmente	*11*	*61,1*	*77,8*
Sim	*4*	*22,2*	*100,0*
Total	***19***	***100,0***	

Tabela D.10 – Distribuição da frequência das respostas da questão 7 da maturidade 1

8 - As interrupções planejadas são programadas para alcançar necessidades da TI, porém, não consideram requisitos do negócio?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*9*	*50,0*	*50,0*
Pouco	*3*	*16,7*	*66,7*
Parcialmente	*3*	*16,7*	*83,3*
Sim	*3*	*16,7*	*100,0*
Total	***19***	***100,0***	

Tabela D.11 – Distribuição da frequência das respostas da questão 8 da maturidade 1

D.3 – Distribuição das frequencias das respostas relacionadas ao nível de maturidade 2 (Repetitivo, mas intuitivo)

1 - A responsabilidade para assegurar continuidade de serviços de TI é formalmente atribuída?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*2*	*10,5*	*10,5*
Pouco	*1*	*5,3*	*15,8*
Parcialmente	*9*	*47,4*	*63,2*
Sim	*7*	*36,8*	*100,0*
Total	***19***	***100,0***	

Tabela D.12 – Distribuição da frequência das respostas da questão 1 da maturidade 2

2 - As estratégias para assegurar continuidade de serviços de TI tratam isoladamente os serviços e sistemas críticos?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*1*	*5,3*	*5,3*
Pouco	*2*	*10,5*	*15,8*
Parcialmente	*6*	*31,6*	*47,4*
Sim	*10*	*52,6*	*100,0*
Total	***19***	***100,0***	

Tabela D.13 – Distribuição da frequência das respostas da questão 2 da maturidade 2

3 - Os relatórios sobre disponibilidade dos sistemas são esporádicos, incompletos e não levam em conta o impacto sobre o negócio?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*2*	*10,5*	*10,5*
Pouco	*0*	*0,0*	*10,5*
Parcialmente	*7*	*36,8*	*47,4*
Sim	*10*	*52,6*	*100,0*
Total	***19***	***100,0***	

Tabela D.14 – Distribuição da frequência das respostas da questão 3 da maturidade 2

4 - Existe compromisso da gerência quanto à continuidade de serviços de TI?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*2*	*10,5*	*10,5*
Pouco	*2*	*10,5*	*21,1*
Parcialmente	*5*	*26,3*	*47,4*
Sim	*10*	*52,6*	*100,0*
Total	***19***	***100,0***	

Tabela D.15– Distribuição da frequência das respostas da questão 4 da maturidade 2

5 - Existe um inventário de sistemas e componentes críticos?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*2*	*11,1*	*11,1*
Pouco	*3*	*16,7*	*27,8*
Parcialmente	*9*	*50,0*	*77,8*
Sim	*4*	*22,2*	*100,0*
Total	***19***	***100,0***	

Tabela D.16 – Distribuição da frequência das respostas da questão 5 da maturidade 2

D.4 – Distribuição das frequencias das respostas relacionadas ao nível de maturidade 3 (Definido)

1 - As responsabilidades para planejamento e teste de continuidade de serviços de TI estão claramente definidas e atribuídas?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*4*	*22,2*	*22,2*
Pouco	*6*	*33,3*	*55,6*
Parcialmente	*6*	*33,3*	*88,9*
Sim	*2*	*11,1*	*100,0*
Total	***19***	***100,0***	

Tabela D.17 – Distribuição da frequência das respostas da questão 1 da maturidade 3

2 - O plano de continuidade de TI está documentado?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*1*	*5,6*	*5,6*
Pouco	*3*	*16,7*	*22,2*
Parcialmente	*3*	*16,7*	*38,9*
Sim	*11*	*61,1*	*100,0*
Total	***19***	***100,0***	

Tabela D.18 – Distribuição da frequência das respostas da questão 2 da maturidade 3

3 - O plano de continuidade de TI é baseado na criticidade do sistema e no impacto do negócio?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*1*	*5,3*	*5,3*
Pouco	*3*	*15,8*	*21,1*
Parcialmente	*5*	*26,3*	*47,4*
Sim	*10*	*52,6*	*100,0*
Total	***19***	***100,0***	

Tabela D.19 – Distribuição da frequência das respostas da questão 3 da maturidade 3

4 - Há um relatório periódico de teste de continuidade de serviços de TI?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*15*	*78,9*	*78,9*
Pouco	*3*	*15,8*	*94,7*
Parcialmente	*1*	*5,3*	*100,0*
Sim	*0*	*0,0*	*100,0*
Total	***19***	***100,0***	

Tabela D.20 – Distribuição da frequência das respostas da questão 4 da maturidade 3

5 - Os indivíduos tomam a iniciativa para o seguimento de padrões e recebimento de treinamento para lidar com incidentes importantes ou um desastre?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*4*	*21,1*	*21,1*
Pouco	*5*	*26,3*	*47,4*
Parcialmente	*9*	*47,4*	*94,7*
Sim	*1*	*5,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.21 – Distribuição da frequência das respostas da questão 5 da maturidade 3

6 - A gerência comunica consistentemente a necessidade de planejamento para assegurar serviço contínuo?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*2*	*10,5*	*10,5*
Pouco	*8*	*42,1*	*52,6*
Parcialmente	*5*	*26,3*	*78,9*
Sim	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela D.22 – Distribuição da frequência das respostas da questão 6 da maturidade 3

7 - Os componentes da alta disponibilidade e da redundância dos sistemas e serviços estão operando corretamente?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*0*	*0,0*	*0,0*
Pouco	*1*	*5,3*	*5,3*
Parcialmente	*8*	*42,1*	*47,4*
Sim	*10*	*52,6*	*100,0*
Total	***19***	***100,0***	

Tabela D.23 – Distribuição da frequência das respostas da questão 7 da maturidade 3

8 - Um inventário de sistemas e componentes críticos é mantido?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*3*	*15,8*	*15,8*
Pouco	*7*	*36,8*	*52,6*
Parcialmente	*8*	*42,1*	*94,7*
Sim	*1*	*5,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.24 – Distribuição da frequência das respostas da questão 8 da maturidade 3

D.5 – Distribuição das frequencias das respostas relacionadas ao nível de maturidade 4 (Gerenciado e Medido)

1 - As responsabilidades e padrões para continuidade de serviços são exigidas da forma como foram definidos?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*2*	*10,5*	*10,5*
Pouco	*10*	*52,6*	*63,2*
Parcialmente	*6*	*31,6*	*94,7*
Sim	*1*	*5,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.25– Distribuição da frequência das respostas da questão 1 da maturidade 4

2 - É atribuída a responsabilidade de manter o plano de continuidade de serviços de TI?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*2*	*10,5*	*10,5*
Pouco	*3*	*15,8*	*26,3*
Parcialmente	*6*	*31,6*	*57,9*
Sim	*8*	*42,1*	*100,0*
Total	***19***	***100,0***	

Tabela D.26 – Distribuição da frequência das respostas da questão 2 da maturidade 4

3 - As atividades de manutenção são baseadas nos resultados de testes de continuidade de serviços de TI, nas boas práticas internas e nas mudanças do ambiente de TI e de negócio?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*6*	*31,6*	*31,6*
Pouco	*6*	*31,6*	*63,2*
Parcialmente	*6*	*31,6*	*94,7*
Sim	*1*	*5,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.27 – Distribuição da frequência das respostas da questão 3 da maturidade 4

4 - Os dados estruturados sobre continuidade de serviços de TI estão sendo reunidos, analisados, reportados e trabalhados?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*9*	*47,4*	*47,4*
Pouco	*5*	*26,3*	*73,7*
Parcialmente	*5*	*26,3*	*100,0*
Sim	*0*	*0,0*	*100,0*
Total	***19***	***100,0***	

Tabela D.28 – Distribuição da frequência das respostas da questão 4 da maturidade 4

5 - É oferecido treinamento formal, de forma obrigatória, sobre os processos de continuidade de serviços de TI?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*10*	*52,6*	*52,6*
Pouco	*5*	*26,3*	*78,9*
Parcialmente	*3*	*15,8*	*94,7*
Sim	*1*	*5,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.29 – Distribuição da frequência das respostas da questão 5 da maturidade 4

6 - As boas práticas da disponibilidade de sistemas e serviços estão sendo aplicadas consistentemente?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*3*	*15,8*	*15,8*
Pouco	*9*	*47,4*	*63,2*
Parcialmente	*5*	*26,3*	*89,5*
Sim	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela D.30 – Distribuição da frequência das respostas da questão 6 da maturidade 4

7 - Os incidentes de descontinuidade são classificados.

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*9*	*47,4*	*47,4*
Pouco	*6*	*31,6*	*78,9*
Parcialmente	*2*	*10,5*	*89,5*
Sim	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela D.31 – Distribuição da frequência das respostas da questão 7 da maturidade 4

8 - O caminho crescente de escalonamento para cada um dos incidentes de descontinuidade é bem conhecido por todos os envolvidos?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*9*	*47,4*	*47,4*
Pouco	*8*	*42,1*	*89,5*
Parcialmente	*1*	*5,3*	*94,7*
Sim	*1*	*5,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.32 – Distribuição da frequência das respostas da questão 8 da maturidade 4

D.6 – Distribuição das frequencias das respostas relacionadas ao nível de maturidade 5 (Otimizado)

1 - Os processos integrados de continuidade de serviços de TI levam em conta as melhores práticas externas?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*4*	*22,2*	*22,2*
Pouco	*7*	*38,9*	*61,1*
Parcialmente	*5*	*27,8*	*88,9*
Sim	*2*	*11,1*	*100,0*
Total	***19***	***100,0***	

Tabela D.33– Distribuição da frequência das respostas da questão 1 da maturidade 5

2 - O plano de continuidade de TI é integrado com os planos de continuidade do negócio?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*8*	*42,1*	*42,1*
Pouco	*3*	*15,8*	*57,9*
Parcialmente	*6*	*31,6*	*89,5*
Sim	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela D.34 – Distribuição da frequência das respostas da questão 2 da maturidade 5

3 - O plano de continuidade de TI é mantido rotineiramente?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*4*	*21,1*	*21,1*
Pouco	*7*	*36,8*	*57,9*
Parcialmente	*7*	*36,8*	*94,7*
Sim	*1*	*5,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.35 – Distribuição da frequência das respostas da questão 3 da maturidade 5

4 - Os requisitos para assegurar continuidade de serviços de TI são apoiados pelos principais fornecedores?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/10)*100*	*Acumulada*
Não	*3*	*16,7*	*16,7*
Pouco	*5*	*27,8*	*44,4*
Parcialmente	*7*	*38,9*	*83,3*
Sim	*3*	*16,7*	*100,0*
Total	***19***	***100,0***	

Tabela D.36 – Distribuição da frequência das respostas da questão 4 da maturidade 5

5 - Ocorre teste global do plano de continuidade de TI?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*15*	*78,9*	*78,9*
Pouco	*2*	*10,5*	*89,5*
Parcialmente	*2*	*10,5*	*100,0*
Sim	*0*	*0,0*	*100,0*
Total	***19***	***100,0***	

Tabela D.37 – Distribuição da frequência das respostas da questão 5 da maturidade 5

6 - Os resultados do teste global são entradas para a atualização do plano de continuidade de serviços de TI?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*17*	*89,5*	*89,5*
Pouco	*0*	*0,0*	*89,5*
Parcialmente	*0*	*0,0*	*89,5*
Sim	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela D.38 – Distribuição da frequência das respostas da questão 6 da maturidade 5

7 - Coleta e análise de dados são usadas para a melhoria contínua do processo?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*8*	*42,1*	*42,1*
Pouco	*6*	*31,6*	*73,7*
Parcialmente	*4*	*21,1*	*94,7*
Sim	*1*	*5,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.39 – Distribuição da frequência das respostas da questão 7 da maturidade 5

8 - Práticas de disponibilidade e planejamento de continuidade de serviços de TI são alinhados completamente?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*8*	*42,1*	*42,1*
Pouco	*6*	*31,6*	*73,7*
Parcialmente	*4*	*21,1*	*94,7*
Sim	*1*	*5,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.40 – Distribuição da frequência das respostas da questão 8 da maturidade 5

9 - A gerência assegura que um desastre ou um incidente importante não ocorra como conseqüência de um ponto único de falha?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/10)*100	***Acumulada***
Não	*6*	*31,6*	*31,6*
Pouco	*5*	*26,3*	*57,9*
Parcialmente	*3*	*15,8*	*73,7*
Sim	*5*	*26,3*	*100,0*
Total	***19***	***100,0***	

Tabela D.41 – Distribuição da frequência das respostas da questão 9 da maturidade 5

APÊNDICE E – MAPEAMENTO DAS FREQUÊNCIAS DAS RESPOSTAS REFERENTES AO NÍVEL DE MATURIDADE DO PROCESSO DS4

Nível de maturidade: 0 Inexistente						
Nº DA QUESTÃO	**QUESTÃO**	**NÃO**	**POUCO**	**PARCIAL**	**SIM**	**VALOR DE CONFORMIDADE DA QUESTÃO**
1	Existe uma percepção dos riscos, vulnerabilidades e ameaças às operações de TI?				X	0
2	Existe uma percepção do impacto da perda de serviços de TI para o negócio?				X	0
3	A continuidade do serviço é considerada necessária pela a administração?				X	0
					Total	**0**
Nível de maturidade: 1 Inicial / Ad hoc						
1	As responsabilidades referentes a continuidade de serviços de TI são informais?			X		0,66
2	A autoridade para execução dos procedimentos de continuidade de serviços de TI é limitada?			X		0,66
3	A gerência tem ciência dos riscos relacionados à continuidade de serviços de TI?				X	1
4	A gerência tem ciência da necessidade da continuidade de serviços de TI?				X	1
5	O foco da atenção do gerenciamento em continuidade de serviços de TI está nos recursos de infraestrutura, ao invés de estar nos serviços de TI?			X		0,66
6	Os usuários implementam procedimentos de contorno em resposta às interrupções de serviços?		X			0,33
7	A resposta da TI às principais interrupções é reativa e despreparada?			X		0,66
8	As interrupções planejadas são programadas para alcançar necessidades da TI, porém, não consideram requisitos do negócio?	X				0
					Total	**4,97**

Nível de maturidade: 2 Repetitivo, mas intuitivo						
1	A responsabilidade para assegurar continuidade de serviços de TI é formalmente atribuída?			X		0,66
2	As estratégias para assegurar continuidade de serviços de TI tratam isoladamente os serviços e sistemas críticos?				X	1
3	Os relatórios sobre disponibilidade dos sistemas são esporádicos, incompletos e não levam em conta o impacto sobre o negócio?				X	1
4	Existe compromisso da gerência quanto a continuidade de serviços de TI?				X	1
5	Existe um inventário de sistemas e componentes críticos?			X		0,66
					Total	**4,32**
Nível de maturidade: 3 Processo Definido						
1	As responsabilidades para planejamento e teste de continuidade de serviços de TI estão claramente definidas e atribuídas?		X			0,33
2	O plano de continuidade de TI está documentado?				X	1
3	O plano de continuidade de TI é baseado na criticidade do sistema e no impacto do negócio?				X	1
4	Há um relatório periódico de teste de continuidade de serviços de TI?	X				0
5	Os indivíduos tomam a iniciativa para o seguimento de padrões e recebimento de treinamento para lidar com incidentes importantes ou um desastre?			X		0,66
6	A gerência comunica consistentemente a necessidade de planejamento para assegurar serviço contínuo?		X			0,33
7	Os componentes da alta disponibilidade e da redundância dos sistemas e serviços estão operando corretamente?				X	1
8	Um inventário de sistemas e componentes críticos é mantido?			X		0,66

					Total	**4,98**
Nível de maturidade: 4 Gerenciado e Medido						
1	As responsabilidades e padrões para continuidade de serviços são exigidas da forma como foram definidos?		X			0,33
2	É atribuída a responsabilidade de manter o plano de continuidade de serviços de TI?				X	1
3	As atividades de manutenção são baseadas nos resultados de testes de continuidade de serviços de TI, nas boas práticas internas e nas mudanças do ambiente de TI e de negócio?	X				0
4	Os dados estruturados sobre continuidade de serviços de TI estão sendo reunidos, analisados, reportados e trabalhados?	X				0
5	É oferecido treinamento formal, de forma obrigatória, sobre os processos de continuidade de serviços de TI?	X				0
6	As boas práticas da disponibilidade de sistemas e serviços estão sendo aplicadas consistentemente?		X			0,33
7	Os incidentes de descontinuidade são classificados?	X				0
8	O caminho crescente de escalonamento para cada um dos incidentes de descontinuidade é bem conhecido por todos os envolvidos?	X				0
					Total	**1,66**
Nível de maturidade: 5 Otimizado						
1	Os processos integrados de continuidade de serviços de TI levam em conta as melhores práticas externas?		X			0,33
2	O plano de continuidade de TI é integrado com os planos de continuidade do negócio?	X				0
3	O plano de continuidade de TI é mantido rotineiramente?		X			0,33
4	Os requisitos para assegurar continuidade de serviços de TI são apoiados pelos principais fornecedores?			X		0,66

5	Ocorre teste global do plano de continuidade de TI?	X				0
6	Os resultados do teste global são entradas para a atualização do plano de continuidade de serviços de TI?	X				0
7	Coleta e análise de dados são usadas para a melhoria contínua do processo?	X				0
8	Práticas de disponibilidade e planejamento de continuidade de serviços de TI são alinhados completamente?	X				0
9	A gerência assegura que um desastre ou um incidente importante não ocorra como conseqüência de um ponto único de falha?				X	
					Total	**1,32**

Tabela E.1 – Mapeamento das frequências das respostas referentes a maturidade do processo DS4.

APÊNDICE F – ANÁLISE DA FREQUÊNCIA DAS QUESTÕES RELACIONADAS AOS OBJETIVOS DE CONTROLE DO PROCESSO DS4

F.1 Análise da frequência do objetivo de controle DS4.1 - Framework de Continuidade de TI

1 - Um processo para gerenciamento da continuidade de serviços de TI foi definido?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*13*	*68,4*	*68,4*
Não	*4*	*21,1*	*89,5*
Não sei	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela F.1 – Distribuição da frequência das respostas da questão 1 do DS4.1

2 - O processo para gerenciamento da continuidade de serviços de TI foi aprovado pela Secretaria de Tecnologia?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*12*	*63,2*	*63,2*
Não	*5*	*26,3*	*89,5*
Não sei	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela F.2 – Distribuição da frequência das respostas da questão 2 do DS4.1

3 - O plano de continuidade de TI definiu claramente os componentes necessários para recuperar os serviços relacionados ao processo eletrônico durante um incidente?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*8*	*42,1*	*42,1*
Não	*7*	*36,8*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.3 – Distribuição da frequência das respostas da questão 3 do DS4.1

4 - O framework de continuidade inclui todos os elementos necessários para restabelecer os serviços de TI, incluindo dentre eles os relacionados ao processo eletrônico, no caso de interrupção (considerando responsabilidades, plano de comunicação, plano de escalação, estratégias de recuperação, níveis de serviço da TI e do negócio, e procedimentos emergenciais)?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*5*	*26,3*	*26,3*
Não	*7*	*36,8*	*63,2*
Não sei	*7*	*36,8*	*100,0*
Total	***19***	***100,0***	

Tabela F.4 – Distribuição da frequência das respostas da questão 4 do DS4.1

F.2 Análise da frequência do objetivo de controle DS4.2 - Planos de Continuidade de TI

1 - Existem planos de continuidade para os sistemas e serviços mais importantes?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*14*	*73,7*	*73,7*
Não	*3*	*15,8*	*89,5*
Não sei	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela F.5 – Distribuição da frequência das respostas da questão 1 do DS4.2

2 - Cada plano de continuidade define formas de processamento alternativo?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*8*	*42,1*	*42,1*
Não	*7*	*36,8*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.6 – Distribuição da frequência das respostas da questão 2 do DS4.2

3 - Cada plano de continuidade define capacidade de recuperação alinhada ao impacto do serviço?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*6*	*31,6*	*31,6*
Não	*8*	*42,1*	*73,7*
Não sei	*5*	*26,3*	*100,0*
Total	***19***	***100,0***	

Tabela F.7 – Distribuição da frequência das respostas da questão 3 do DS4.2

4 - Cada plano define regras e responsabilidades?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*13*	*68,4*	*68,4*
Não	*3*	*15,8*	*84,2*
Não sei	*3*	*15,8*	*100,0*
Total	***19***	***100,0***	

Tabela F.8 – Distribuição da frequência das respostas da questão 4 do DS4.2

5 - Cada plano inclui processos de comunicação?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*11*	*57,9*	*57,9*
Não	*3*	*15,8*	*73,3*
Não sei	*5*	*26,3*	*100,0*
Total	***19***	***100,0***	

Tabela F.9 – Distribuição da frequência das respostas da questão 5 do DS4.2

6 - Cada plano define uma configuração de recuperação mínima aceitável?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*7*	*36,8*	*36,8*
Não	*5*	*26,3*	*63,2*
Não sei	*7*	*36,8*	*100,0*
Total	***19***	***100,0***	

Tabela F.10 – Distribuição da frequência das respostas da questão 6 do DS4.2

7 - Existe uma estratégia de testes para os planos de continuidade?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*5*	*26,3*	*26,3*
Não	*10*	*52,6*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.11 – Distribuição da frequência das respostas da questão 7 do DS4.2

8 - Os testes dos planos de continuidade estão sendo executados em uma freqüência combinada entre as áreas?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*1*	*5,3*	*5,3*
Não	*16*	*84,2*	*89,5*
Não sei	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela F.12 – Distribuição da frequência das respostas da questão 8 do DS4.2

9 - Os resultados dos testes são analisados?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*1*	*5,3*	*5,3*
Não	*14*	*73,7*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.13 – Distribuição da frequência das respostas da questão 9 do DS4.2

F.3 Análise da frequência do objetivo de controle DS4.3 - Recursos Críticos de TI

1 - Existe um inventário dos serviços e sistemas e seus respectivos níveis de criticidade?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*8*	*42,1*	*42,1*
Não	*9*	*47,4*	*89,5*
Não sei	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela F.14 – Distribuição da frequência das respostas da questão 1 do DS4.3

2 - Os sistemas e serviços mais críticos possuem planos de continuidade, suportando processos e recursos?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*13*	*68,4*	*68,4*
Não	*4*	*21,1*	*89,5*
Não sei	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela F.15 – Distribuição da frequência das respostas da questão 2 do DS4.3

3 - Os planos de continuidade foram definidos de acordo com os objetivos do negocio e conformidade legal?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*9*	*47,4*	*47,4*
Não	*6*	*31,6*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.16 – Distribuição da frequência das respostas da questão 3 do DS4.3

4 - Os planos de continuidade foram testados de acordo com os objetivos do negocio e conformidade legal?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*4*	*21,1*	*21,1*
Não	*10*	*52,6*	*73,7*
Não sei	*5*	*26,3*	*100,0*
Total	***19***	***100,0***	

Tabela F.17 – Distribuição da frequência das respostas da questão 4 do DS4.3

5 - Existe um processo para assegurar a consistência entre os vários planos de continuidade dos sistemas e serviços críticos?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*4*	*21,1*	*21,1*
Não	*8*	*42,1*	*63,2*
Não sei	*7*	*36,8*	*100,0*
Total	***19***	***100,0***	

Tabela F.18 – Distribuição da frequência das respostas da questão 5 do DS4.3

F.4 Análise da frequência do objetivo de controle DS4.4 - Manutenção do Plano de Continuidade de TI

1 - Todas as cópias do plano de continuidade de TI são revisadas e atualizadas periodicamente?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*10*	*52,6*	*52,6*
Não	*4*	*21,1*	*73,7*
Não sei	*5*	*26,3*	*100,0*
Total	***19***	***100,0***	

Tabela F.19 – Distribuição da frequência das respostas da questão 1 do DS4.4

2 - Todas as cópias são armazenadas on-site e off-site?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*7*	*36,8*	*36,8*
Não	*3*	*15,8*	*52,6*
Não sei	*9*	*47,7*	*100,0*
Total	***19***	***100,0***	

Tabela F.20 – Distribuição da frequência das respostas da questão 2 do DS4.4

3 - Todas as mudanças criticas dos recursos de TI são comunicadas para o gerente de continuidade para atualização do plano de continuidade?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*5*	*26,3*	*26,3*
Não	*10*	*52,6*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.21 – Distribuição da frequência das respostas da questão 3 do DS4.4

4 - As mudanças no plano de continuidade são realizadas em intervalos regulares?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*6*	*31,6*	*31,6*
Não	*9*	*47,4*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.22 – Distribuição da frequência das respostas da questão 4 do DS4.4

5 - As mudanças no plano de continuidade seguem procedimentos de controle de alteração?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*10*	*52,6*	*52,6*
Não	*3*	*15,8*	*68,4*
Não sei	*6*	*31,6*	*100,0*
Total	***19***	***100,0***	

Tabela F.23 – Distribuição da frequência das respostas da questão 5 do DS4.4

F.5 Análise da frequência do objetivo de controle DS4.5 - Teste do Plano de Continuidade de TI

1 - Os testes de continuidade de TI são agendados e aplicados regularmente após alterações da infraestrutura de TI e das aplicações?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*2*	*10,5*	*10,5*
Não	*14*	*73,7*	*84,2*
Não sei	*3*	*15,8*	*100,0*
Total	***19***	***100,0***	

Tabela F.24 – Distribuição da frequência das respostas da questão 1 do DS4.5

2 - Novos componentes e atualizações são incluídos no agendamento de testes do plano de continuidade?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*5*	*26,3*	*26,3*
Não	*12*	*63,2*	*89,5*
Não sei	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela F.25 – Distribuição da frequência das respostas da questão 2 do DS4.5

3 - Um agendamento de teste foi criado e inclui detalhes do teste para garantir uma seqüência lógica e real das interrupções?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*0*	*0,0*	*0,0*
Não	*14*	*73,7*	*73,3*
Não sei	*5*	*26,3*	*100,0*
Total	***19***	***100,0***	

Tabela F.26 – Distribuição da frequência das respostas da questão 3 do DS4.5

4 - Uma equipe para realizar testes foi definida?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*4*	*21,1*	*21,1*
Não	*12*	*63,2*	*84,2*
Não sei	*3*	*15,8*	*100,0*
Total	***19***	***100,0***	

Tabela F.27 – Distribuição da frequência das respostas da questão 4 do DS4.5

5 - As pessoas envolvidas nos testes são diferentes daquelas responsáveis pela execução do plano de continuidade?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*2*	*10,5*	*10,5*
Não	*9*	*47,4*	*57,9*
Não sei	*8*	*42,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.28 – Distribuição da frequência das respostas da questão 5 do DS4.5

6 - É verificada junto à equipe a definição de uma alternativa quando os testes não são viáveis?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*4*	*21,1*	*21,1*
Não	*9*	*47,4*	*68,4*
Não sei	*6*	*31,6*	*100,0*
Total	***19***	***100,0***	

Tabela F.29 – Distribuição da frequência das respostas da questão 6 do DS4.5

7 - O sucesso ou falha do teste é medido e reportado e a mudança é realizada no plano de continuidade?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*3*	*15,8*	*15,8*
Não	*10*	*52,6*	*68,4*
Não sei	*6*	*31,6*	*100,0*
Total	***19***	***100,0***	

Tabela F.30 – Distribuição da frequência das respostas da questão 7 do DS4.5

8 - Os resultados são revisados para determinar a eficácia da operação?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*3*	*15,8*	*15,8*
Não	*10*	*52,6*	*68,4*
Não sei	*6*	*31,6*	*100,0*
Total	***19***	***100,0***	

Tabela F.31 – Distribuição da frequência das respostas da questão 8 do DS4.5

F.6 Análise da frequência do objetivo de controle DS4.6 - Treinamento do Plano de Continuidade de TI

1 - São realizados treinamentos referentes aos procedimentos de continuidade de serviços regularmente?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*1*	*5,3*	*5,3*
Não	*16*	*84,2*	*89,5*
Não sei	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela F.32 – Distribuição da frequência das respostas da questão 1 do DS4.6

2 - A necessidade de treinamento e o agendamento são avaliados e atualizados regularmente?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*1*	*5,3*	*5,3*
Não	*12*	*63,2*	*68,4*
Não sei	*6*	*31,6*	*100,0*
Total	***19***	***100,0***	

Tabela F.33– Distribuição da frequência das respostas da questão 2 do DS4.6

3 - A lista, agendamento e material de treinamento são revisados para determinar a eficácia da operação?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*3*	*15,8*	*15,8*
Não	*14*	*73,7*	*89,5*
Não sei	*2*	*10,5*	*100,0*
Total	***19***	***100,0***	

Tabela F.34– Distribuição da frequência das respostas da questão 3 do DS4.6

4 - Programas para divulgar projetos de continuidade de TI estão sendo realizados em todos os níveis?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*1*	*5,3*	*5,3*
Não	*14*	*73,7*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.35– Distribuição da frequência das respostas da questão 4 do DS4.6

F.7 Análise da frequência do objetivo de controle DS4.7 - Distribuição do Plano de Continuidade de TI

1 - Uma lista de distribuição para o plano de continuidade de TI foi definida?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*10*	*52,6*	*52,6*
Não	*5*	*26,3*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.36 – Distribuição da frequência das respostas da questão 1 do DS4.7

2 - O procedimento de distribuição foi avaliado?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*5*	*26,3*	*26,3*
Não	*7*	*36,8*	*63,2*
Não sei	*7*	*36,8*	*100,0*
Total	***19***	***100,0***	

Tabela F.37 – Distribuição da frequência das respostas da questão 2 do DS4.7

3 - Todas as cópias digitais e físicas do plano estão protegidas?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*8*	*42,1*	*42,1*
Não	*4*	*21,1*	*63,2*
Não sei	*7*	*36,8*	*100,0*
Total	***19***	***100,0***	

Tabela F.38 – Distribuição da frequência das respostas da questão 3 do DS4.7

4 - Os documentos são acessados somente por pessoas autorizadas?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*10*	*52,6*	*52,6*
Não	*3*	*15,8*	*68,4*
Não sei	*6*	*31,6*	*100,0*
Total	***19***	***100,0***	

Tabela F.39– Distribuição da frequência das respostas da questão 4 do DS4.7

F.8 Análise da frequência do objetivo de controle DS4.8 - Recuperação e Retomada de Serviços de TI

1 - Para os casos de incidente, os procedimentos incluem todos os passos para a avaliação dos danos, bem como trata dos pontos formais de decisões necessários para a ativação dos planos de continuidade?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*9*	*47,4*	*47,7*
Não	*5*	*26,3*	*73,7*
Não sei	*5*	*26,3*	*100,0*
Total	***19***	***100,0***	

Tabela F.40 – Distribuição da frequência das respostas da questão 1 do DS4.8

2 - Os planos de recuperação correspondem aos requisitos do negócio?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*8*	*42,1*	*42,1*
Não	*3*	*15,8*	*57,9*
Não sei	*8*	*42,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.41 – Distribuição da frequência das respostas da questão 2 do DS4.8

F.9 Análise da frequência do objetivo de controle DS4.9 - Armazenamento do backup em outros locais

1 - Os dados estão protegidos quando estão em um sistema de armazenamento offsite?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*11*	*57,9*	*57,9*
Não	*4*	*21,1*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.42 – Distribuição da frequência das respostas da questão 1 do DS4.9

2 - Os dados estão protegidos quando transportados?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*4*	*21,1*	*21,1*
Não	*11*	*57,9*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.43 – Distribuição da frequência das respostas da questão 2 do DS4.9

3 - Os dados estão protegidos quando estão no local de armazenamento alternativo?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*12*	*63,2*	*63,2*
Não	*3*	*15,8*	*78,9*
Não sei	*4*	*21,1*	*100,0*
Total	***19***	***100,0***	

Tabela F.44 – Distribuição da frequência das respostas da questão 3 do DS4.9

4 - Os procedimentos de teste foram revisados para determinar a eficácia da operação?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*2*	*10,5*	*10,5*
Não	*8*	*42,1*	*52,6*
Não sei	*9*	*47,4*	*100,0*
Total	***19***	***100,0***	

Tabela F.45 – Distribuição da frequência das respostas da questão 4 do DS4.9

5 - A mídia de backup contém toda a informação necessária para o plano de continuidade de TI?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*5*	*26,3*	*26,3*
Não	*1*	*5,3*	*31,6*
Não sei	*13*	*68,4*	*100,0*
Total	***19***	***100,0***	

Tabela F.46 – Distribuição da frequência das respostas da questão 5 do DS4.9

6 - Existem instruções de recuperação suficientes?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*7*	*36,8*	*36,8*
Não	*6*	*31,6*	*68,4*
Não sei	*6*	*31,6*	*100,0*
Total	***19***	***100,0***	

Tabela F.47 – Distribuição da frequência das respostas da questão 6 do DS4.9

7 - Existe um inventário dos backups e mídias?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*13*	*68,4*	*68,4*
Não	*0*	*0,0*	*68,4*
Não sei	*6*	*31,6*	*100,0*
Total	***19***	***100,0***	

Tabela F.48 – Distribuição da frequência das respostas da questão 7 do DS4.9

8 - É verificado se esse inventário está correto?

Resposta	*Frequência Absoluta (A)*	*Frequência relativa (%)*	
		*Simples (A/19)*100*	*Acumulada*
Sim	*6*	*31,6*	*31,6*
Não	*0*	*0,0*	*31,6*
Não sei	*13*	*68,4*	*100,0*
Total	***19***	***100,0***	

Tabela F.49 – Distribuição da frequência das respostas da questão 8 do DS4.9

F.10 Análise da frequência do objetivo de controle DS4.10 - Revisão Pós-retomada

1 - As falhas do plano se tornam focos importantes para a adequação e atualização do plano de continuidade?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*4*	*21,1*	*21,1*
Não	*9*	*47,4*	*68,4*
Não sei	*6*	*31,6*	*20,0*
Total	***19***	***100,0***	

Tabela F.50 – Distribuição da frequência das respostas da questão 1 do DS4.10

2 - Após efetuar recuperações, são realizadas reuniões para discutir melhorias?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*4*	*21,1*	*21,1*
Não	*10*	*52,6*	*73,7*
Não sei	*5*	*26,3*	*100,0*
Total	***19***	***100,0***	

Tabela F.51 – Distribuição da frequência das respostas da questão 2 do DS4.10

3 - Planos, políticas e procedimentos foram revisados para determinar a eficácia da operação?

Resposta	***Frequência Absoluta (A)***	***Frequência relativa (%)***	
		Simples (A/19)*100	***Acumulada***
Sim	*6*	*31,6*	*31,6*
Não	*10*	*52,6*	*84,2*
Não sei	*3*	*15,8*	*100,0*
Total	***19***	***100,0***	

Tabela F.52– Distribuição da frequência das respostas da questão 3 do DS4.10